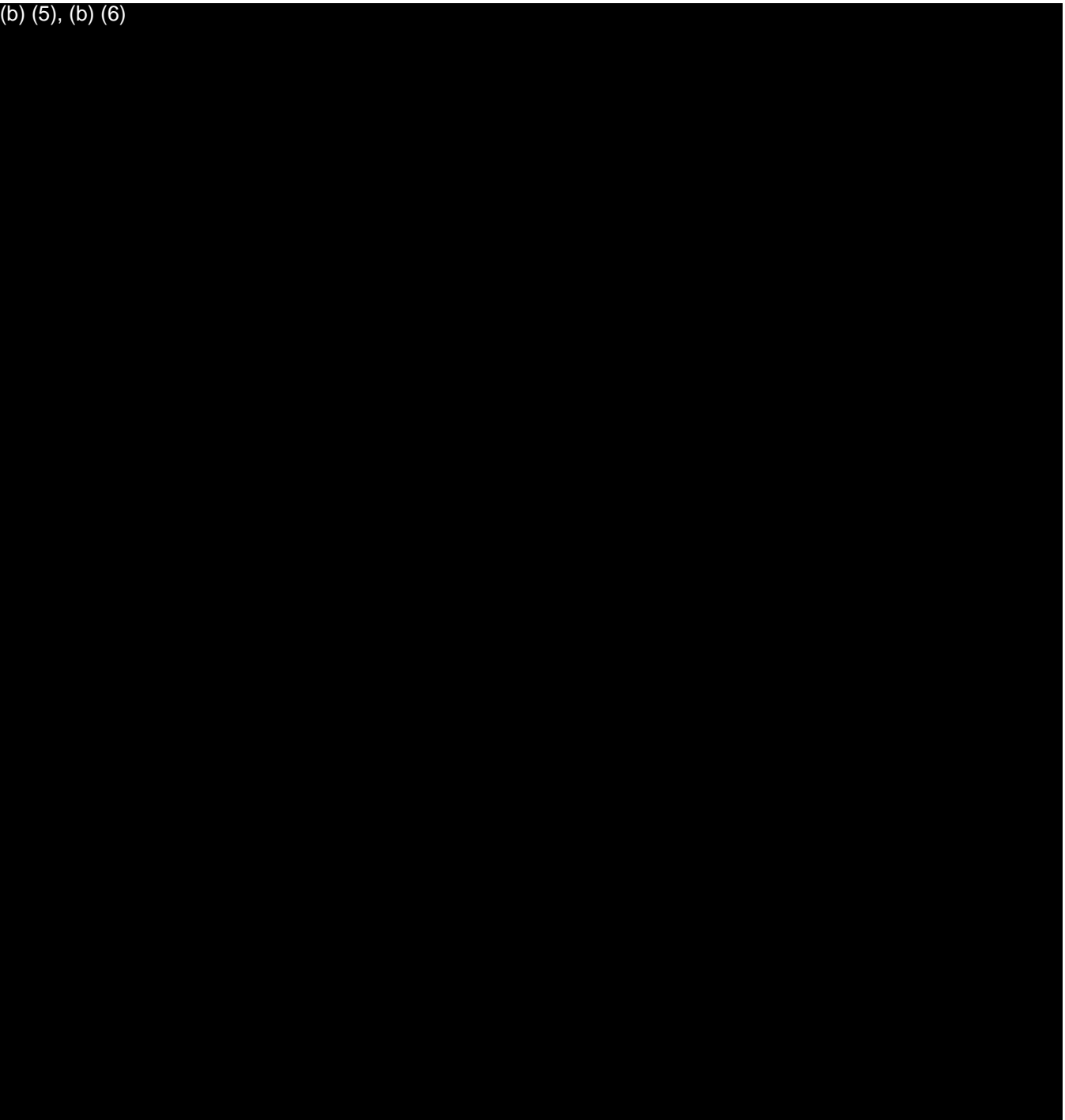


(b) (5), (b) (6)



From: POLITICO Pro Cybersecurity Whiteboard [<mailto:politicoemail@politicopro.com>]

Sent: Wednesday, March 29, 2017 12:54 PM

To: (b) (6)

Subject: DHS creating election security coordinating group

By Eric Geller

03/29/2017 12:43 PM EDT

The Department of Homeland Security is beginning to set up a coordinating body for election

cybersecurity consultations with state officials, a DHS official said today.

“We are doing that work now,” Neil Jenkins, the director of DHS’s enterprise performance management office, said at a meeting of the technical standards agency NIST’s cyber advisory group. “That work is in the planning phases, and we’re beginning outreach to” election administrators and voting system vendors.

At the end of the Obama administration, following Russia’s alleged cyberattack campaign and intrusions at two state election offices, DHS designated election systems as "critical infrastructure," on par with hospitals and the power grid. In making its designation, DHS created a new election subsector under the existing government facilities sector, one of the 16 critical infrastructure sectors.

Sectors and subsectors are managed through coordinating councils, which include representatives from affected critical infrastructure operators, technical experts and consulting federal agencies.

DHS and state officials will meet several times in the next few weeks to begin planning an election security coordinating council, Jenkins said at the NIST meeting. “We’re starting to engage with them more robustly.”






The department will spend the next few months showing state election officials how coordinating councils work in the private sector, Jenkins said.

“Our goal is to have a robust sector built up for them ... at the end of this year or beginning of next year,” he added, “so that we can be doing this in the lead-up to the November 2018 elections.”

To view online:

<https://www.politicopro.com/cybersecurity/whiteboard/2017/03/dhs-creating-election-security-coordinating-group-085616>

Was this Pro content helpful? Tell us what you think in one click.

				
Yes. very	Somewhat	Neutral	Not really	Not at all

You received this POLITICO Pro content because your customized settings include: tags: Cybersecurity: Executive Branch, Cybersecurity: Vulnerabilities, Cybersecurity: Breaches, Cybersecurity: States/Governors, Cybersecurity: Critical Infrastructure, Cybersecurity: Department Of Homeland Security. To change your alert settings, please go to <https://www.politicopro.com/settings>

This email was sent by: POLITICO, LLC
1000 Wilson Blvd. Arlington, VA, 22209, USA

Cyber Vigilance: The Virginia Way

National Cyber "Firsts" are Second Nature in Virginia

National Institute of Standards and Technology (NIST) Cyber Framework: First in the nation to adopt federal standards

Information Sharing and Assessment Organization (ISAO): First state to declare itself an ISAO

Securing Consumer Transactions: First state to require security on debit or credit card present transactions, via Executive Directive #5

Digital Identity: First state to enact landmark legislation, now used as the model by other states

Virginia Apprenticeship Program: for the first time in Virginia history, businesses have the opportunity to stand up registered apprenticeships for cyber security occupations



"Few issues are more fundamental to the security and prosperity of the Commonwealth and its citizens than the safe, reliable, and secure operation of our computer networks and the systems they enable."

COMMONWEALTH OF VIRGINIA
CYBER SECURITY COMMISSION

First Report, Aug. 2015

Cyber Policy Leadership

Executive Order #8 Launches Cyber Virginia and the Cyber Security Commission

Executive Directive #6 Improved cyber protocols, expanded cyber related risk management activities and conducted inventory of the Commonwealth's critical and sensitive systems

HB1946/SB919 Sealing of administrative subpoenas for electronic communications and social networking data

SB1307 Clarifies language for search warrants for seizure, examination of computers, networks, and other electronic devices

SB1109 Secures FOIA exemptions for meetings and discussions which include sensitive information regarding cybersecurity vulnerabilities

SB1129 Secures FOIA exemptions for plans, information, or responses to terrorism regarding cybersecurity threats and vulnerabilities

SB1121 Defines IT responsibilities of agency directors

HB1562/SB814 Electronic identity management standards; liability

HB924 Allows providers to verify the authenticity of reports or records with an affidavit from the custodian of the records

Open Cyber
Jobs in Virginia

17,000

Average Cyber
Starting Salary in Virginia

\$88,000

Average salary in
Virginia with a Certified
Information Systems
Security Professional (CISSP)
designation

\$93,010

CYBER JOBS: VIRGINIA CYBER FIRMS ARE HIRING!
Virginia is second only to California in its cyber workforce size

Cyber Attacks Thwarted In the Commonwealth

The Cyber Security Commission recognizes two national trends that will create additional needs in cybersecurity focused on cyber-physical systems:

1. Rapidly growing initiatives in advanced automation of physical systems (e.g., UAS' automated control of automobiles, digital factories, 3D printers, "Internet of Things")
2. Cyber attacks have been growing in frequency and sophistication, which can cause physical and economic harm to existing kinetic systems.

In order to adequately address the security concerns for these systems, security must be built in from the beginning through inherently secure design. **This creates an opportunity for Virginia businesses and universities to invest in research in these areas of growth in our economy.**

53,517,902

Attack attempts (4 per second)

353,032,453

Spam messages blocked

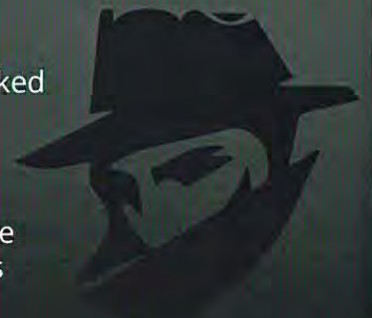
42,187

Pieces of malware blocked

131

Attack attempts became cyber security incidents

Data collected January - May 2016



CYBER INNOVATION

Virginia Writes the Book Daily

MACH37: Innovative accelerator for emerging security firms. To date Mach37 has launched 35 cyber security companies in Virginia; www.mach37.com

Virginia Cyber Security Partnership: Established by Governor McAuliffe; researches technologies to safeguard citizens and agencies from cyber attacks against smart vehicles

Cyber Portal: Public website provides reputable information on cyber standards and best practices for citizens, businesses, and government organizations; www.cyberva.virginia.gov

CYBER EDUCATION

Virginia is Training its Workforce Now

Through a rigorous certification process, the U.S. National Security Agency and Department of Homeland Security certify post-secondary schools that excel in cyber defense training as "Cyber Defense, Centers of Academic Excellence."

Innovative cyber training to speed worker readiness for the New Virginia Economy:

- **Cyber Boot Camps:** Cyber Education training for high school teachers
- **Conference on Cyber and Education:** Discussion and education on the importance of training for cyber careers
- **Cyber Range:** Secure platform built for training, research & collaboration

Cyber Defense, Centers of Academic Excellence

George Mason University
Hampton University*
James Madison University
Longwood University
Marymount University
Norfolk State University
Virginia Polytechnic Institute*
Radford University
Northern Virginia Community College
Lord Fairfax Community College
Tidewater Community College

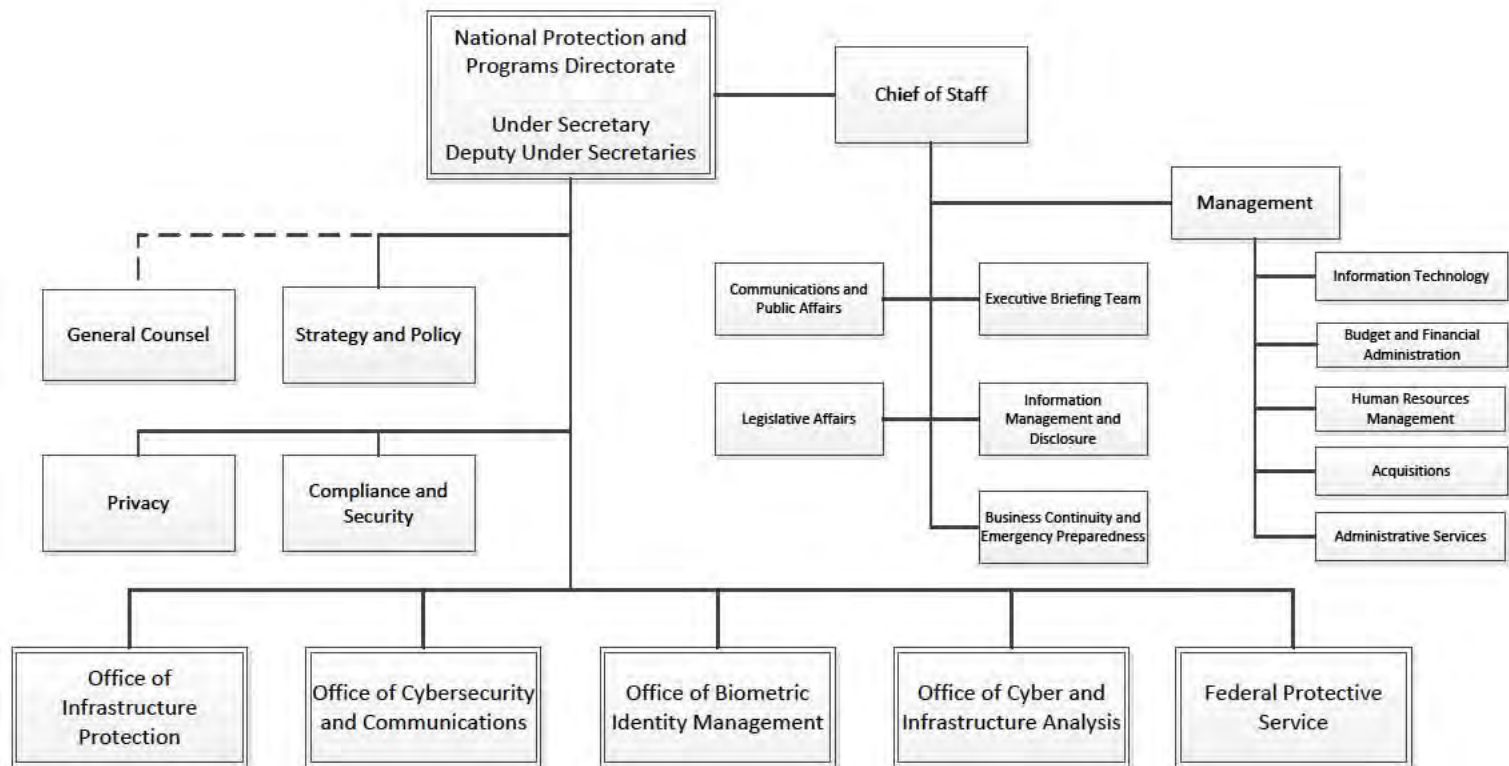
* Denotes two Cyber Centers of Academic Excellence

New Virginia Cyber Security Agenda

- 1 Increase the number of Cyber Defense, Centers of Academic Excellence
- 2 Virginia Scholarship for Service Program
- 3 Veterans Pathway Program in Cyber Security at GMU
- 4 Virginia Cyber Range
- 5 Information Sharing and Analysis Organization
- 6 Virginia Fusion Center

FOR MORE INFORMATION

visit <http://cyberva.virginia.gov> or call 804-786-9579





Homeland Security Starts with Hometown Security

The U.S. Department of Homeland Security (DHS) closely monitors attacks on public gatherings and public places to constantly enhance the Nation's security. During both steady state and times of heightened awareness, DHS engages closely with our private sector and community partners to provide expert counsel and recommendations about protective measures they can implement to protect facilities and venues. DHS provides free tools and resources to communities because the Department recognizes that communities are the first line of defense in keeping the public safe and secure.

The Department encourages businesses to Connect, Plan, Train, and Report. Applying these four steps in advance of an incident or attack can help better prepare businesses and their employees to proactively think about the role they play in the safety and security of their businesses and communities.

CONNECT: Reach out and develop relationships in your community, including local law enforcement. Having these relationships established before an incident occurs can help speed up the response when something happens.

- Develop relationships with local law enforcement and businesses in your area. Invite local law enforcement to tour your business.
- Connect with community security and preparedness organizations such as the Federal Bureau of Investigation's public-private partnership program "InfraGard."
- Contact the local DHS Protective Security Advisor who is available to support your efforts.
- Communicate with your customers and let them know about the security measures you are taking to ensure a positive experience and to maintain public safety.
- If your business is located at or near a Federal facility, connect with DHS's Federal Protective Service at 1-877-4FPS-411.

PLAN: Take the time now to plan on how you will handle a security event should one occur. Learn from other events to inform your plans.

- Be aware of current threats related to your geographic region or impacting your business sector.
- Develop plans, including security, emergency response, emergency communications, and business continuity plans, while considering the protection of your employees and customers, access control, closed-circuit television, signage, suspicious activity reporting, and parking security.
- Evaluate your security requirements and design a monitoring, surveillance, and inspection program that is consistent with your business operations.
- Develop evacuation and shelter-in-place plans, and ensure that multiple evacuation routes are clearly marked with appropriate signage and that rallying points are available.
- Develop and implement a security plan for computer and information systems hardware and software.

- Engage local first responders (police, fire, medical) in all of the above efforts to ensure your efforts are in synergy with theirs.

TRAIN: Provide your employees with training resources and exercise your plans often. The best laid plans must be exercised in order to be effective.

- Train employees on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device (IED). Ensure they understand security basics, emergency response, business continuity plans, and increased awareness of potential threats.
- Exercise your emergency communications plan.

REPORT: “If You See Something, Say Something™” is more than just a slogan. Call local law enforcement.

- Post details on reporting suspicious activity and encourage employees, tenants, and visitors to report suspicious behavior to property management security or local law enforcement. Things to consider include unattended vehicles; repeat visitors or outsiders who have no apparent business in non-public area; abandoned parcels, suitcases, backpacks, and packages; and other unusual activity.
- Get involved with the Department’s “If You See Something, Say Something™” campaign.

DHS Programs, Resources, and Tools You Can Use

Protective Security Advisors proactively engage with government partners and the private sector to protect critical infrastructure. For more information or to contact your local PSA, e-mail NICC@hq.dhs.gov.

The Ready Campaign provides help with planning for businesses at <http://www.ready.gov/business>.

DHS Active Shooter resources are available at <http://www.dhs.gov/active-shooter-preparedness>.

“If You See Something, Say Something™” <http://www.dhs.gov/see-something-say-something>.

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) information is available at <https://nsi.ncirc.gov/>. SAR training for private sector partners is located at https://nsi.ncirc.gov/hsptregistration/private_sector/.

Counter-Improvised Explosive Device information and resources are available at www.dhs.gov/tripwire.

Information on **DHS cybersecurity programs** is available at www.dhs.gov/cyber. To find out more about the Cybersecurity Awareness Campaign, go to <http://www.dhs.gov/stopthinkconnect>. For tips from the U.S. Computer Emergency Response Team, go to <https://www.us-cert.gov/ncas/tips>.

InfraGard is a public-private partnership between the FBI and the private sector that represents individuals from businesses, academic institutions, State and local law enforcement, and fire and EMS agencies, as well as other participants dedicated to sharing information, education, and intelligence. Please go to www.infragardmembers.org and <https://www.infragard.org>.



Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to



systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact

Threat Response

Asset Response

Federal Bureau of Investigation (FBI)

FBI Field Office Cyber Task Forces:

<http://www.fbi.gov/contact-us/field>

Internet Crime Complaint Center (IC3):

<http://www.ic3.gov>

Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.

Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.

National Cyber Investigative Joint Task Force

NCIJTF CyWatch 24/7 Command Center: (855) 292-3937
or cywatch@ic.fbi.gov

Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.

United States Secret Service

Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):

<http://www.secretservice.gov/contact/field-offices>

Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information

United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)

HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or
<https://www.ice.gov/webform/hsi-tip-form>

HSI Field Offices: <https://www.ice.gov/contact/hsi>

HSI Cyber Crimes Center: <https://www.ice.gov/cyber-crimes>

Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov

United States Computer Emergency Readiness Team:

<http://www.us-cert.gov>

Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

If there is an immediate threat to public health or safety, the public should always call 911.



NATIONAL CYBER INCIDENT RESPONSE PLAN

December 2016



**Homeland
Security**

This page intentionally left blank.

Table of Contents

EXECUTIVE SUMMARY	4
INTRODUCTION.....	6
SCOPE	6
GUIDING PRINCIPLES.....	7
RELATIONSHIP TO NATIONAL PREPAREDNESS SYSTEM.....	8
ROLES AND RESPONSIBILITIES.....	10
CONCURRENT LINES OF EFFORT	11
THREAT RESPONSE	12
Private Sector.....	12
State, Local, Tribal, and Territorial Governments	13
Federal Government	13
ASSET RESPONSE.....	14
Private Sector.....	14
State, Local, Tribal, and Territorial Government.....	16
Federal Government	17
INTELLIGENCE SUPPORT	19
State, Local, Tribal, and Territorial Government.....	19
Federal Government	20
AFFECTED ENTITY’S RESPONSE	21
Cyber Incidents Involving Personally Identifiable Information	21
CORE CAPABILITIES	21
Access Control and Identity Verification	22
Cybersecurity.....	22
Forensics and Attribution.....	22
Infrastructure Systems.....	23
Intelligence and Information Sharing.....	23
Interdiction and Disruption.....	23
Logistics and Supply Chain Management.....	24
Operational Communications	24
Operational Coordination	24
Planning	24
Public Information and Warning.....	25
Screening, Search, and Detection.....	25
Situational Assessment.....	25
Threats and Hazards Identification.....	25
COORDINATING STRUCTURES AND INTEGRATION.....	26
COORDINATING STRUCTURES.....	26
Private Sector.....	26
State, Local, Tribal, and Territorial Governments	27
Federal Government	28
International	29
OPERATIONAL COORDINATION DURING A SIGNIFICANT CYBER INCIDENT	29
Determination of Incident Severity	29
Enhanced Coordination Procedures.....	31
Cyber UCG	31
Information Sharing During Cyber Incident Response.....	34

CONCLUSION 34
ANNEX A: AUTHORITIES AND STATUTES..... 36
ANNEX B: CYBER INCIDENT SEVERITY SCHEMA..... 38
**ANNEX C: CYBER INCIDENT SEVERITY SCHEMA/ NATIONAL RESPONSE
COORDINATION CENTER ACTIVATION CROSSWALK..... 39**
ANNEX D: REPORTING CYBER INCIDENTS TO THE FEDERAL GOVERNMENT 40
ANNEX E: ROLES OF FEDERAL CYBERSECURITY CENTERS 43
ANNEX F: CORE CAPABILITIES AND CRITICAL TASKS..... 45
ANNEX G: DEVELOPING AN INTERNAL CYBER INCIDENT RESPONSE PLAN 53
**ANNEX H: CORE CAPABILITY/NIST CYBERSECURITY FRAMEWORK/PPD-41
CROSSWALK..... 54**
ANNEX I: ADDITIONAL RESOURCES 59
ANNEX J: ACRONYM LIST 60

Executive Summary

Networked technologies touch every corner of the globe and every facet of human life. They have driven innovation, nurtured freedoms, and spurred economic prosperity. Even so, the very technologies that enable these benefits offer new opportunities for malicious and unwanted cyber activities. The risks associated with the Nation's dependence on these networked technologies led to the development of Presidential Policy Directive 41 (PPD-41): *United States Cyber Incident Coordination*, which sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities.

PPD-41 recognizes that the frequency of cyber incidents is increasing, and this trend is unlikely to be reversed anytime soon. The most significant of these incidents, those likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people, necessitate deliberative planning, coordination, and exercising of response activities, in order to minimize the threat and consequences to the Nation, infrastructure, and way of life.

The National Cyber Incident Response Plan (NCIRP or Plan) was developed according to the direction of PPD-41 and leveraging doctrine from the National Preparedness System to articulate the roles and responsibilities, capabilities, and coordinating structures that support how the Nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure. The NCIRP is not a tactical or operational plan; rather, it serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations. Authored in close coordination with government and private sector partners, the NCIRP expounds upon the concurrent lines of effort, defined by PPD-41, for how the Federal Government will organize its activities to manage the effects of significant cyber incidents. The concurrent lines of effort are threat response, asset response, intelligence support, and the affected entity, which undertakes efforts to manage the effects of the incident on its operations, customers, and workforce. The activities and lead federal agencies for each line of effort within the Cyber Unified Coordination Group are described below.

- The Department of Justice is the lead agency for threat response during a significant cyber incident, acting through the Federal Bureau of Investigations and National Cyber Investigative Joint Task Force. Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.
- The Department of Homeland Security is the lead agency for asset response during a significant cyber incident, acting through the National Cybersecurity and Communications Integration Center. Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and

operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

- Threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing guidance to affected entities on available federal resources and capabilities; promptly disseminating through appropriate channels intelligence and information learned in the course of the response; and facilitating information sharing and operational coordination with other Federal Government entities.
- The Office of the Director of National Intelligence is the lead coordinator for intelligence support during a significant cyber incident, acting through the Cyber Threat Intelligence Integration Center. Intelligence support and related activities include providing support to federal asset and threat agencies and facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.
- An affected federal agency shall engage in a variety of efforts to manage the impact of a cyber incident, which may include maintaining business or operational continuity; addressing adverse financial impacts; protecting privacy; managing liability risks; complying with legal and regulatory requirements (including disclosure and notification); engaging in communications with employees or other affected individuals; and dealing with external affairs (e.g., media and congressional inquiries). The affected federal agency will have primary responsibility for this line of effort.
- When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant sector-specific agency will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

The NCIRP builds upon these lines of effort to illustrate a national commitment to strengthening the security and resilience of networked technologies and infrastructure. This Plan outlines the structure and content from which stakeholders can leverage to inform their development of agency-, sector-, and organization-specific operational response plans. Correspondingly, this Plan should be understood to be a living document, to be updated as needed to incorporate lessons-learned, to reflect opportunities and challenges that arise as technology evolves, and to ensure the Plan adequately addresses a changing threat/hazard environment.

Introduction

The *National Cybersecurity Protection Act of 2014* (NCPA)¹ consequently codified in the *Homeland Security Act*², mandates that the Department of Homeland Security (DHS), in coordination with appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure. Presidential Policy Directive (PPD)-41: *U.S. Cyber Incident Coordination* and the associated Annex,³ set forth principles governing the Federal Government's response to any cyber incident, provide an architecture for coordinating the response to significant cyber incidents, and required DHS to develop a National Cyber Incident Response Plan (NCIRP or Plan) to address cybersecurity risks to critical infrastructure. The NCIRP is part of the broader National Preparedness System and establishes the strategic framework and doctrine for a whole-of-Nation⁴ approach to mitigating, responding to, and recovering from a cyber incident. This approach includes and strongly relies on public and private partnerships to address major cybersecurity risks to critical infrastructure.

- **Response Plan Purpose and Organization** – The NCIRP provides guidance to enable a coordinated whole-of-Nation approach to response activities and coordination with stakeholders during a significant cyber incident impacting critical infrastructure. The NCIRP sets common doctrine and a strategic framework for national, sector, and individual organization cyber operational plans.
- **Intended Audience** – The intended audience for the NCIRP is U.S. organizations. However, it may also enhance our international partners' understanding of the U.S. cyber incident coordination. This whole-of-Nation concept focuses efforts and enables the full range of stakeholders—the private and nonprofit sectors (including private and public owners and operators of critical infrastructure), state, local, tribal, territorial (SLTT) governments, and the Federal Government—to participate and be full partners in incident response activities. Government resources alone cannot meet all the needs of those affected by significant cyber incidents. All elements of the community must be activated, engaged, and integrated to respond to a significant cyber incident.

Scope

Cyber incident response is an important component of information and communications technology (ICT) and operational technology programs and systems. Performing incident response effectively is a complex undertaking and requires substantial planning and resources to establish a successful incident response capability.

The NCIRP is the strategic framework for operational coordination among federal and SLTT governments, the private sector, and international partners. Developed according to the guiding principles outlined in PPD-41 and leveraging doctrine from the National Preparedness System and

¹ The National Cybersecurity Protection Act of 2014. Public Law 113-282. December 18, 2014)). <https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf>.

² 6 U.S.C § 149

³ PPD-41: *U.S. Cyber Incident Coordination*. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>; Annex for Presidential Policy Directive-41--United States Cyber Incident Coordination. <https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident>.

⁴ The whole-of-Nation approach also encompasses a wide range of new and existing public and private partnerships to leverage as a platform in working towards managing cybersecurity threats and hazards to critical infrastructure.

the National Incident Management System (NIMS),⁵ the NCIRP sets the strategic framework for how the Nation plans, prepares for, and responds to cyber incidents by establishing an architecture for coordinating the broader community response during a significant cyber incident in accordance with U.S. law and policy. A list of authorities is found in Annex A: Authorities and Statutes. The NCIRP is also designed to integrate and interface with industry standards and best practices for cybersecurity risk management, as developed by the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity.⁶

The NCIRP is not a tactical or operational plan for responding to cyber incidents. However, it should serve as the primary strategic framework for stakeholders when developing agency-, sector-, and organization-specific operational plans. This Plan will help those affected by cyber incidents understand how federal departments and agencies and other national-level partners provide resources to support SLTT and private sector response operations. It should also serve as the basis for national cyber operational playbooks and individual critical infrastructure sector operational coordination plans, as well as be referenced by individual entities in their own plan development. In all cases, incident response activities will be conducted in accordance with applicable law and policy.

Guiding Principles

The NCIRP is based on several guiding principles outlined in PPD-41 for the response to any cyber incident, whether involving government or private sector entities. These principles include:

- **Shared Responsibility.** Individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.
- **Risk-Based Response.** The Federal Government will determine its response actions and the resources it brings to bear based on an assessment of the risks posed to an entity, our national security, foreign relations, the broader economy, public confidence, privacy and civil liberties, or the public health and safety of the American people. Critical infrastructure entities also conduct risk-based response calculations during cyber incidents to ensure the most effective and efficient utilization of resources and capabilities.
- **Respecting Affected Entities.** To the extent permitted under law, Federal Government responders will safeguard details of the incident, as well as privacy, civil liberties, and sensitive private sector information, and generally will defer to affected entities in notifying other affected private sector entities and the public. In the event of a significant cyber incident where the Federal Government interest is served by issuing a public statement concerning an incident, federal responders will coordinate their approach with the affected entities to the extent possible.
- **Unity of Governmental Effort.** Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyber incidents. These entities must coordinate efforts to achieve optimal results. The first federal agency to become aware of a cyber incident will rapidly notify other relevant federal agencies to facilitate a unified federal response and ensure that the right combination of agencies responds to a particular incident. When responding to a cyber incident in the private sector, unity of effort synchronizes the overall federal response, which prevents gaps in service and duplicative efforts. SLTT governments also have responsibilities, authorities, capabilities, and resources that can be

⁵ NIMS. <http://www.fema.gov/national-incident-management-system>.

⁶ Framework for Improving Critical Infrastructure Cybersecurity, version 1.0. National Institute of Standards and Technology, February 12, 2014. <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

used to respond to a cyber incident; therefore, the Federal Government must be prepared to partner with SLTT governments in its cyber incident response efforts. The transnational nature of the Internet and communications infrastructure requires the United States to coordinate with international partners, as appropriate, in managing cyber incidents.

- **Enabling Restoration and Recovery.** Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible.

While steady-state activities and the development of a common operational picture are key components of the NCIRP, the Plan focuses on building the mechanisms needed to respond to a significant cyber incident. Table 1 below describes the difference between a “cyber incident” and a “significant cyber incident” as outlined in PPD-41. The Federal Government uses the Cyber Incident Severity Schema (detailed in Annex B: Cyber Incident Severity Schema) to describe the incident level, the process to determine the severity of an incident, and the threshold for designating a significant cyber incident affecting the United States or its interest abroad. The United States Computer Emergency Readiness Team (US-CERT) website also provides a list of types of common ways cyber incidents can occur and exploit information and assets.⁷

Table 1: Cyber Incident Definitions from PPD-41

Incident	Definition
Cyber Incident	An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
Significant Cyber Incident	A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

Relationship to National Preparedness System

While the NCIRP focuses on cyber incident response efforts, the National Preparedness System outlines a broader architecture that establishes how the broader community⁸ prevents, protects against, mitigates, responds to, and recovers from all threats and hazards. Specifically, the National

⁷ <https://www.us-cert.gov/incident-notification-guidelines#attack-vectors-taxonomy>

⁸ The Response Federal Interagency Operational Plan, Second Edition, August 2016, describes the whole community and includes all individuals and household members, specifically inclusive of people with disabilities, children, older Americans, people with different levels of language English proficiency, communities, the private and nonprofit sectors, faith-based organizations, and local, state, tribal, territorial, insular area, and the Federal Government—and the Nation as a whole. https://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf

Response Framework (NRF)⁹ sets the doctrine and provides guidance for how the Nation builds, sustains, and delivers the response core capabilities identified in the National Preparedness Goal.¹⁰ To further connect the NCIRP with the NRF, the Homeland Security Act¹¹ states the Secretary of DHS, in coordination with the heads of other appropriate federal departments and agencies, and in accordance with the NCIRP under that Act, shall regularly update, maintain, and exercise the Cyber Incident Annex to the NRF of the Department. The NCIRP leverages the doctrine, capabilities, and organizing structures of the NRF, and both the NRF and NCIRP structures align with NIMS as described below.

NIMS provides the common language and incident management structure for government at all levels (federal and SLTT) and the private sector, and defines standard command and management structures. Successful response efforts, including cyber incident responses, depend on a common, interoperable approach for sharing resources, coordination, and communicating information. NIMS defines this comprehensive approach and enables the whole-of-Nation¹² to work together to prevent, protect against, mitigate, respond to, and recover from the effects of incidents regardless of cause, size, location, or complexity.

All of the components of the NIMS—resource management, management and coordination, and communications and information management—provide a common framework by which jurisdictions and organizations, which vary in authorities, management structures, communication capabilities, and protocols, integrate with one another to achieve common goals. These concepts can also apply to cyber incident response, in that they address:

- The development of a single set of incident objectives;
- The use of a collective, strategic approach to incident management;
- The improvement of information flow and coordination;
- The creation of a common understanding of joint priorities and limitations;
- The need to maintain an agency’s legal authorities; and
- The optimization of the combined efforts of all participants in the incident.

The NRF also includes 14 Emergency Support Functions (ESF)¹³; these federal coordinating structures group resources and capabilities into functional areas that are most frequently needed in a national response. ESFs are an effective way to bundle and manage resources to deliver the core capabilities outlined in the NRF. These ESFs bring together the capabilities of federal departments and agencies and other national-level assets to support incident response. The ESFs are not based on

⁹ The NRF is one of five frameworks in the National Preparedness System; it describes how the whole community works together to achieve the National Preparedness Goal within the Response mission area.

<http://www.fema.gov/national-response-framework>.

¹⁰ <http://www.fema.gov/national-preparedness-goal>.

¹¹ 6 U.S.C. § 149

¹² The National Preparedness System refers to whole community vs the NCIRP describing a whole-of-Nation approach because of the nature of cyber infrastructure and associated incidents. The guidance, programs, processes, and systems that support each component of the National Preparedness System enable a collaborative, whole community approach to national preparedness that engages individuals, families, communities, private and nonprofit sectors, faith-based organizations, and all levels of government. <https://www.fema.gov/media-library-data/20130726-1855-25045-8110/national-preparedness-system-final.pdf>

¹³ <http://www.fema.gov/national-preparedness-resource-library>.

the capabilities of any single department or agency but are groups of organizations that work together to support an effective response.

Activation of the ESFs, either by the DHS Federal Emergency Management Agency (FEMA) or as directed by the Secretary of Homeland Security, depends upon the response activities needed to support the incident. Specifically, through ESF #2 (Communications), the Federal Government can coordinate the response to and recovery from a significant cyber incident that also creates large-scale physical effects with the communications sector and across the other ESFs. In an incident with cyber and physical effects, the significant cyber incident response mechanism outlined in the Coordinating Structures and Integration section of this Plan will coordinate with the established ESFs, to include ESF #2. A graphic comparing the Cyber Incident Severity Schema and Activation Level of the National Response Coordination Center is provided in Annex C. This center is a multiagency center that coordinates the overall federal support for major incidents and emergencies.¹⁴

The next section describes the concurrent lines of effort outlined in PPD-41 and identifies key roles and responsibilities for not only the federal and SLTT governments' response but also the private sectors' response to a cyber incident as they own and operate the bulk of the Nations' critical infrastructure.

Roles and Responsibilities

Every day, various organizations across the public and private sectors manage, respond to, and investigate cyber incidents through concurrent lines of effort. Fostering unity of effort during incident response requires a shared understanding of the roles and responsibilities of all participating organizations, to include roles that may be unique or particularly relevant for protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.

The Federal Government maintains a wide range of capabilities and resources that may be required to respond to a cyber incident, many of them through its cybersecurity centers which are further described in Annex E: Roles of Federal Cybersecurity Centers. In responding to any cyber incident and recognizing the shared responsibility for cybersecurity, the Federal Government organizes its' response activities based upon four concurrent lines of effort: threat response, asset response, intelligence support, and the affected entity's internal response activities.

When a cyber incident affects a private entity, the Federal Government will typically not play a direct role in the affected entities' response activities but will remain cognizant of their activities and coordinate appropriately with the affected entity. Where possible, and especially where incidents may escalate on the Cyber Incident Severity Schema, the Federal Government will conduct coordinated outreach efforts with the affected entity and offer to assist with asset response, threat response, and intelligence support activities, consistent with the guiding principles described in the Scope section of this Plan.

Cyber incidents can result from the actions, or inactions, of a single individual. When engaged and educated, individuals, families, and households can greatly reduce the impact, disruption, and damage caused by a cyber event. While most cyber incidents may not involve assistance from private citizens, incidents can reduce the risk and potential impact of a cyber incident to their personal property. Resources and guidance are available at www.ready.gov/cyber-attack that private citizens

¹⁴ The National Response Coordination Center. https://www.fema.gov/media-library-data/1440617086835-f6489d2de59dddeba8bebc9b4d419009/NRCC_July_2015.pdf

can leverage before, during, and after a cyber incident. US-CERT also provides information to home users on security risks and countermeasures associated with home Internet connectivity.¹⁵

Concurrent Lines of Effort

Recognizing the shared responsibility for cybersecurity, response activities in the NCIRP are undertaken through three concurrent lines of effort: threat response, asset response, intelligence support and related activities. A fourth line of effort is the affected entity’s response efforts.¹⁶ These concurrent lines of effort provide a foundation for harmonizing various response efforts and fostering coordination and unity of effort before, during, and after any cyber incident response. Federal and non-federal entities should remain cognizant of these lines of effort and facilitate their activities accordingly while responding to cyber incidents.

Table 2. Lead Federal Agencies During Significant Cyber Incidents Affecting Civilian Networks¹⁷

Line of Effort	Lead Federal Agency
Threat Response	Department of Justice (DOJ) through the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF)
Asset Response	Department of Homeland Security (DHS) through National Cybersecurity and Communications Integration Center (NCCIC)
Intelligence Support	Office of the Director of National Intelligence (ODNI) through Cyber Threat Intelligence Integration Center (CTIIC)
Affected Entity Response	When a significant cyber incident affects a federal agency, that agency will have primary responsibility for its response. When a significant cyber incident affects a private entity, the Federal Government will typically not play a role in this line of effort, but the cognizant Sector Specific Agency(ies) will generally coordinate the Federal Government efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

Threat and asset responders share some responsibilities and activities, including but not limited to:

- Communicating with the affected entity to understand the nature of the cyber incident;
- Providing guidance to the affected entity on available federal resources and capabilities;
- Promptly disseminating, through appropriate channels, intelligence and information learned in the course of the response; and
- Facilitating information sharing and operational coordination with other entities.

International coordination plays a key role through all the lines of effort. Due to the transnational nature of the Internet and communications infrastructure, and the global presence and connectivity of

¹⁵ <https://www.us-cert.gov/Home-Network-Security>

¹⁶ PPD-41: U.S. Cyber Incident Coordination. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

¹⁷ Per the Annex to PPD-41, asset and threat response activities for significant cyber incidents affecting DoD or IC assets are led by those agencies with support from other federal agencies as appropriate. Lead agencies also coordinate with relevant SSAs, if a cyber incident affects or is likely to affect sectors they represent.

the U.S. private sector, the Federal Government may coordinate with international partners in response to all aspects of a cyber incident—threat response, asset response, and intelligence support.

The Department of State (DOS) represents the United States in all global diplomatic engagements across the full range of international policy imperatives, including cyber issues. As stated in the 2011 International Strategy for Cyberspace, diplomacy is a vital and necessary component to addressing cyber threats and responding to cyber incidents both domestically and internationally. DOS leverages its diplomats in the embassies and posts around the globe to provide international diplomatic support for cyber incident response around the clock. While DOS coordinates diplomatic outreach related to cyber incidents, many federal departments and agencies actively maintain and leverage multilateral and bilateral partnerships. Similarly, many ICT sector businesses and providers are multinational businesses with critical international elements and relationships, including interaction with both policy and operational communities around the world. As appropriate, federal departments and agencies collaborate internationally and with private sector entities to support international aspects of cyber incident response.

Threat Response

Threat response activities encompass many resources and capabilities from across the law enforcement and defense community. Threat response activities during a cyber incident include investigative, forensic, analytical, and mitigation activities; interdiction of a threat actor; and providing attribution that may lead to information sharing and operational synchronization with asset response activities. Threat response activities also include conducting appropriate law enforcement and national security investigative activities at the affected entity's site, linking related incidents, and identifying additional affected or potentially affected entities. As described earlier, threat responders and asset responders collaborate to foster a unity of effort to facilitate their activities while responding to incidents. The SLTT community and the private sector play important roles in working with respective law enforcement entities on threat response activities. Federal agencies with counterintelligence functions, such as those of DHS, DOJ, DoD, Department of Energy (DOE), and members of the Intelligence Community (IC), may perform a substantial threat response role when a significant cyber incident affects their duties or responsibilities, or there is suspicion of activities conducted a foreign power or agent of a foreign power.

Private Sector

Private sector entities perform critical roles in supporting threat response activities by reporting and sharing information regarding cyber incidents and malicious cyber activity in a timely manner to appropriate law enforcement agencies or government entities. Information, communications, and technology providers and manufacturers—such as Internet service providers, common carriers, manufacturers of key networking hardware, and major software companies—also play an important role in the threat response to malicious cyber activity, due to the potential exploitation or use of their systems by cyber threat actors. Points of contact for reporting incidents to Federal Government entities are provided in Annex D: Reporting Cyber Incidents to the Federal Government. Private sector entities should also adhere to regulatory and legal requirements when reporting cyber incidents. Private sector cybersecurity practitioners and providers that offer critical services (such as managed security services, indications and warning, cybersecurity assessment, and incident response) may also possess information concerning malicious cyber activity that is important to enable threat response activities. The *Cybersecurity Information Sharing Act of 2015* provides liability and other legal protections to private sector and certain SLTT government organizations and establishes

important conditions regarding sharing information with the Federal Government, SLTT government organizations, and the private sector.¹⁸

State, Local, Tribal, and Territorial Governments

Many states and locals have criminal statutes regarding unauthorized access or damage to computer systems, which could be implicated in a cyber incident. State fusion centers are situated at the intersection between federal and local law enforcement, and play a role in sharing threat-related information between federal, SLTT and/or private sector partners. However, state fusion centers vary greatly in their cyber capacity and capability. Local governments, particularly large cities, play an important role in local response activities. Often times, private citizens and small businesses do not have relationships with or access to federal law enforcement or in incident response activities. Local governments have a critical responsibility to provide a communication bridge to federal and state law enforcement and incident responders. As identified in the previous sub-section (Private Sector), the *Cybersecurity Information Sharing Act of 2015* establishes legal protections and important conditions for sharing information with the Federal Government, SLTT government organizations, and the private sector.

Federal Government

In response to cyber incidents, federal law enforcement agencies work across SLTT and the Federal Government, international engagements, and with private sector entities to address both criminal and national security cyber threats. Federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI), United States Secret Service (U.S. Secret Service), and U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), conduct threat response activities related to criminal activity involving their investigative jurisdictions and coordinate appropriately. Sharing action information in an unclassified format between the IC and first responders is critical in coordinating incident response activities.

Pursuant to PPD-41, during the event of a significant cyber incident for which a Cyber Unified Coordination Group (UCG) is convened, the DOJ, through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), will serve as the lead federal agency for threat response activities. The specific responsibilities and coordinating roles for this line of effort during a significant cyber incident are detailed in the Operational Coordination During a Significant Cyber Incident section of this Plan.

DOJ's Offices of U.S. Attorneys and its' Criminal and National Security Divisions, working with federal law enforcement agencies, use criminal and national security authorities to investigate, prosecute, and disrupt cyber threats and to apprehend cyber threat actors. Information and evidence obtained pursuant to appropriate legal process are used to identify the source of cyber incidents and to gather pertinent cyber threat information. Nationwide coordination of cyber prosecutorial initiatives is conducted through the DOJ Computer Hacking and Intellectual Property Program for criminal matters and by the DOJ National Security Cyber Specialist Network for cyber threats to the national security. In addition, DOJ, through the FBI and NCIJTF, shares investigative information and cyber threat intelligence, as appropriate, with other federal agencies to aid in the analysis of cyber threats and vulnerabilities. The FBI Cyber Task Forces in all 56 field offices support SLTT

¹⁸ Further information and guidance to assist non-federal entities to share cyber threat indicators and defensive measures with federal entities under the Cybersecurity Information Sharing Act of 2015 can be found at <https://www.us-cert.gov/ais>.

law enforcement in maintaining relationships and sharing information with the private sector, offering training and certification courses, and coordination of domestic cyber threat investigations.

The U.S. Secret Service has a national network of Electronic Crimes Task Forces, which combine the resources of academia, the private sector, and SLTT law enforcement to prevent, detect, and investigate electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

DoD is responsible for threat response to cyber incidents affecting DoD assets and the DoD Information Network (DoDIN). DoD can also support civil authorities for cyber incidents outside the DoDIN when requested by the lead federal agency, and approved by the appropriate DoD official, or directed by the President. Such support would be provided based upon the needs of the incident, the capabilities required, and the readiness of available forces.

Asset Response

Asset response activities include furnishing technical assistance to affected entities, mitigating vulnerabilities, identifying additional at-risk entities, and assessing their risk to the same or similar vulnerabilities. These activities could also include communicating with the affected entity to understand the nature of the cyber incident; providing guidance to the affected entity on available federal, SLTT, and private sector resources and capabilities; promptly disseminating new intelligence and information through the appropriate channels; and facilitating information sharing and operational coordination with other Federal Government, SLTT government, and private sector entities. Critical asset response activities also include assessing potential risks to a sector or region, including potential cascading and interdependency effects, developing courses of action to mitigate these risks, and providing guidance on how best to utilize federal, SLTT, and private sector resources and capabilities in a timely, effective manner.

Asset and threat responders coordinate and share some responsibilities and activities when responding to a cyber incident. The roles and responsibilities in asset response vary, which highlights that unity of effort and shared responsibility is necessary to protect the Nation against cyber incidents.

Private Sector

The private sector, especially the owners and operators of critical infrastructure, plays a key role in responding to cyber incidents. Small, medium, and large private sector entities are often the first and primary responders to cyber incidents. Private companies are responsible for the security of their own systems, and they are normally the first to identify an incident and are often in the best place to respond to it. Private entities may have reporting or disclosure requirements related to cyber incidents, which they have to comply with as they respond to the incident. In most cases, these incidents are considered routine and are mitigated by the company using internal resources or with the assistance of contracted services providers. Routine, steady-state information sharing related to cyber incidents, even when mandatory reporting is not required, alerts other at-risk entities and allows them to mitigate vulnerabilities that may have cascading impacts to their systems.

Private sector service providers and cybersecurity practitioners offer critical services, such as managed security services, indications and warning, cybersecurity assessment, and incident response, which system owners and other asset responders might need when managing an incident. These private sector resources can serve as surge and specialty support to augment an in-house cybersecurity team at an affected entity.

Information, communications, and technology providers and manufacturers, such as Internet service providers, other common carriers, manufacturers of key networking hardware, and major software

companies, play an important role in defending against and responding to malicious cyber activity. Effective coordination between these private sector entities and other response organizations is often essential in cyber incident response.

Critical infrastructure owners and operators work with DHS and relevant sector-specific agencies (SSA) implementing the National Infrastructure Protection Plan (NIPP)¹⁹ tenets of public-private partnership to improve preparedness and manage risk. Due to the tightly interconnected and interdependent nature of some sectors, companies may also provide information to other entities in the sector or in other sectors, to facilitate shared situational awareness, contain the incident, and/or mitigate any damage. Thus, companies will potentially look to share and receive information from a variety of sources including DHS, SSAs, and federal and SLTT law enforcement and counterintelligence activities as well as their respective sector Information Sharing Analysis Centers (ISAC) and other information sharing and analysis organizations.

Most private sector operational information sharing is conducted through ISACs. ISACs are typically a sector-based type of Information Sharing and Analysis Organization (ISAO) and operate through a defined sector-based model, meaning that organizations within a certain sector (i.e. financial services, energy, aviation, etc.) join together to share information about cyber threats. Although many of these groups are already essential drivers of effective cybersecurity collaboration, some organizations do not fit neatly within an established sector or have unique needs. ISAOs can be formed based upon geography, sector, or any other grouping in which companies are interested and is a group created to gather, analyze, and disseminate cyber threat information. Those organizations that cannot join an ISAC but have a need for cyber threat information could benefit from membership in an ISAO. Unlike ISACs, ISAOs are not necessarily tied to critical infrastructure sectors.²⁰

In the case of cyber incidents, especially significant cyber incidents, greater coordination may be needed with the Federal Government, SLTT communities, regulators within the sector, and among multiple sectors. In addition to responding to situations in which private companies are themselves the victims of cyber incidents, private entities also respond to situations in which private sector service providers (especially Internet service providers, managed security service providers, and other technology vendors) provide support for national-level incident response efforts. During such an incident, the private sector often provides support or assistance to federal and SLTT departments and agencies on preparedness and response activities. Federal and SLTT regulators also have mandatory reporting requirements for certain types of cyber incidents in certain sectors. Depending on the sector and type of incident, some response actions may require regulator coordination, approval, and/or regulatory relief.

As appropriate, private sector entities provide for the security of their networks and security processing of breaches or other incidents through standing in-house or contracted services or use of external experts. Standing services are a part of the entity's network structure, and the private sector entity are encouraged share with government responders the information the standing services develop or pursue concerning a cyber incident. The *Cybersecurity Information Sharing Act of 2015* provides liability and other legal protections to private sector and certain SLTT government organizations and establishes important conditions regarding sharing information with the Federal Government, SLTT government organizations, and the private sector.²¹

¹⁹ NIPP, 2013. <https://www.dhs.gov/national-infrastructure-protection-plan>.

²⁰ <https://www.dhs.gov/isao-faq>

²¹ Further information and guidance to assist non-federal entities to share cyber threat indicators and defensive measures with federal entities under the Cybersecurity Information Sharing Act of 2015 can be found at <https://www.us-cert.gov/ais>.

State, Local, Tribal, and Territorial Government

Ensuring the safety and welfare of citizens is a fundamental responsibility of government at every level. Toward these objectives, key executives, executive leadership, elected officials, and executive staff of each SLTT government are responsible for ensuring preparedness, response, and recovery activities within their jurisdiction.

In cases of cyber incidents, the standard emergency response roles and responsibilities may not be sufficient to address technical challenges. Each state is responsible for developing a plan that describes their role in asset response for entities within their state. This state plan should be consistent with the NCIRP and serve as a cyber annex to their respective state emergency management plan. Information described in Annex G: Developing an Internal Cyber Incident Response Plan provides information each state can consider when developing a cyber incident response plan that coordinates identifying, detecting, mitigating, responding to, and recovering from cyber incidents in their state.

In establishing strong governance and reporting mechanisms, executives should identify key individual response points-of-contact for their respective governments and ensure the Federal Government has the most up-to-date information for these individuals. To facilitate coordination during a significant cyber incident response operation, each key executive should pre-designate a primary individual to serve as Senior Official to represent its government. Until amended, by each key executive, the NCCIC uses the state Homeland Security Advisors as its primary point of contact.

Governance is vital and an enabling factor in states' cyber asset response role. This includes the supporting legal framework, policies, plans, and procedures that codify the state chief information security officer's authorities and responsibilities. Governance also outlines how these relate to executive branch departments and agencies, and other state-operated entities to include (and not limited to) state and local emergency management functions, law enforcement, the judicial and legislative branches, ports, airports, and other state owned critical infrastructure. As identified in the previous sub-section (Private Sector), the *Cybersecurity Information Sharing Act of 2015* establishes legal protections and important conditions for sharing information with the Federal Government, SLTT government organizations, and the private sector.

Resources available to SLTT communities include, but are not limited to, the following:

- Regional Homeland Security Offices and Fusion Centers;
- Multi-State ISAC (MS-ISAC) is funded through grants from DHS to support the security of the SLTT government networks²² and acts as a focal point for critical information exchange and coordination between the SLTT community and the Federal Government; every state has an MS-ISAC primary member, usually the state chief information security officer (CISO);
- Local governments that are eligible to apply and receive Urban Area Security Initiative grant funds are encouraged to include cybersecurity and training programs as part of their expenditures.
- DHS National Protection and Programs Directorate field personnel, including:

²² The MS-ISAC does not help SLTT governments who are seeking to support the private sector. If an SLTT government is supporting a private sector company in asset response, the SLTT government should engage directly with the NCCIC.

- Supervisory, regional, and district-level Cybersecurity Advisors, who work closely with SLTT Chief Information Security Officers and cyber emergency management communities as cybersecurity subject matter experts;
- Regional directors and Protective Security Advisors, who work closely with state homeland security advisors as critical infrastructure protection specialists;
- The Governors Homeland Security Advisors Council, which provides a structure through which homeland security advisors from each state, territory, and the District of Columbia discuss homeland security issues, share information and expertise, and keep governors informed of the issues affecting homeland security policies in the states;
- The SLTT Government Coordinating Councils (SLTT GCC), which strengthen the sector partnership structure by bringing together geographically diverse experts from a wide range of critical infrastructure disciplines to ensure that SLTT officials play an integral role in national critical infrastructure security and resilience efforts.

The National Guard is a force with dual state and federal roles. National Guard forces have expertise in critical response functions and many also have expertise and capabilities in cyber activities. At the direction of a State Governor and Adjutant General, the National Guard may perform state missions, including supporting civil authorities in response to a cyber incident. In certain circumstances, as permitted by law, the National Guard may be requested to perform federal service or be ordered to active duty to perform DoD missions, which could include supporting a federal agency in response to a cyber incident.

Following a cyber incident, SLTT community leaders and points of contact may be asked to provide advice, support, and assistance to federal departments and agencies on preparedness and response activities related to SLTT priorities. Cyber incidents can cause cascading and/or physical impacts that implicate non-cyber incident response activities by SLTT governments. Key executives and points of contact have a need for situational awareness of the Federal Government’s asset response activities even when a cyber incident does not affect the SLTT government systems. They should be prepared to request additional resources from the Federal Government—for instance, under the Stafford Act—in the event of a cyber incident that exceeds their government’s capabilities.

Federal Government

Federal asset response to a significant cyber incident encompasses many resources and capabilities from across the federal departments and agencies as well as with the private sector. In response to cyber incidents, the Federal Government works with both domestic and foreign partners, including both private sector and governmental entities, to assist in assessments, mitigation, recovery, and restoration activities. Pursuant to PPD-41, in the event of a significant cyber incident for which a Cyber UCG is convened, DHS, through the NCCIC, will serve as the lead federal agency for asset response activities. The specific responsibilities and coordinating roles for this line of effort during a significant cyber incident are detailed in the Operational Coordination During a Significant Cyber Incident section of this Plan.

The Office of Management and Budget and the Federal Information Security Modernization Act of 2014 directs federal departments and agencies to report major cyber incidents within seven days as well as submitting to Congress, DHS, and Office of Management and Budget on an annual basis.²³

²³ Federal Information Security Modernization Act of 2014. Public Law No: 113-283. December 18, 2014. <https://www.congress.gov/bill/113th-congress/senate-bill/2521>

DHS, through the US-CERT, must be notified of all computer security incidents involving a Federal Government information system with a confirmed impact to confidentiality, integrity, or availability within one hour of being positively identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center, or Information Technology department.²⁴

DHS provides strategic guidance, promotes a national unity of effort, and coordinates the overall federal effort to promote the security and resilience of the Nation's critical infrastructure from cyber and other threats.²⁵ Per the NCPA, DHS, through the NCCIC, serves as the federal civilian interface for sharing information related to cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities.²⁶ The NCCIC facilitates information sharing to help identify other entities at risk to the same or similar vulnerabilities and shares mitigation recommendations and best practices to protect those at risk. The NCCIC closely coordinates with the SSAs, representatives from multiple agencies, and the private sector to share cybersecurity information, information about risks and incidents, analysis, and warnings among federal and non-federal entities, and to facilitate coordination regarding cybersecurity risks and incidents across the civilian communities, SLTT governments, and the private sector. Federal asset response support to the private sector from the NCCIC in the form of on-site technical assistance is generally contingent on a request from or consent of the supported entity.

SSAs also play a role in sector coordination, working closely with DHS and serving as a day-to-day federal interface to prioritize and coordinate activities within their respective sectors; carrying out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations; and providing support or facilitating technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate. DHS ensures consistent and integrated approaches across various critical infrastructure sectors, and a nationwide approach including both unity of effort and unity of messages.

DHS, working with relevant SSAs, also coordinates the Government's efforts to understand the potential business or operational impact of a cyber incident on critical infrastructure in a given sector and across sectors. The relevant SSA will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure. SSAs receive support from the DHS NCCIC and the National Infrastructure Coordinating Center to maintain and provide situational awareness on threats, incidents, or events impacting critical infrastructure and to facilitate information sharing. This includes a near-real-time capability to provide SSA reports, coordinated with FEMA ESF reporting provided by the National Response Coordination Center, and the capability to solicit and receive information on incidents from public and private sector critical infrastructure partners. Because SSAs often have authorities, responsibilities, and partnerships with private industry that extend beyond security and resilience issues, SSAs play a lead role in integrating response to the technical aspects of cybersecurity incidents with efforts to mitigate the systemic impacts of such incidents to sectors.

²⁴ US-CERT Federal Incident Notification Guidelines. <https://www.us-cert.gov/incident-notification-guidelines>

²⁵ Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. February 12, 2013. PPD-12 also assigns roles and responsibilities to other federal agencies. The Department of Justice and Federal Bureau of Investigation lead counterterrorism and counterintelligence investigations and related law enforcement activities across critical infrastructure. The Department of Homeland Security and the Attorney General collaborate to carry out their respective missions in critical infrastructure. <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

²⁶ The National Cybersecurity Protection Act of 2014. Public Law 113-282. December 18, 2014. <http://www.gpo.gov/fdsys/pkg/PLAW-113publ282/pdf/PLAW-113publ282.pdf>.

In responding to cyber incidents, DHS also works with foreign partners to exchange information and coordinate incident response activities. This international coordination principally occurs between the NCCIC and its foreign government CSIRT counterparts and builds on regular information sharing and operational coordination relationships. The DOC coordinates with federal, international, and private sector partners on the impacts of cyber incidents on the Internet ecosystem: the domain name system and the digital economy platform representatives to assess those impacts. Through the National Telecommunications and Information Administration and NIST, DOC serves as the Nation's authority on cybersecurity risk management practices and also fulfills responsibilities under the Defense Production Act²⁷ through the Bureau of Industry and Security, including support to critical infrastructure.

In some cases, regulatory or contract requirements could impose certain obligations on the affected entity related to asset response support, such as mandatory reporting requirements and/or national security determinations that may override normal consultative processes. Additionally, where they have relevant authority, federal regulators should be engaged early in the incident response process to ensure that actions requiring waiver or other approval or notification can be quickly executed. Regulators may also be able to facilitate coordinated actions of their respective sectors as necessary during significant cyber incidents.

DoD will be responsible for managing the asset response affected military assets and the DoDIN. DoD can also support civil authorities in responding to cyber incidents outside the DoDIN through a Defense Support of Civil Authorities request based upon a request by the lead federal agency and approved by the appropriate DoD official or directed by the President. Support would be provided based on the needs of the incident, the capabilities required, and the readiness of available forces.

When incidents affect IC assets, the IC Security Coordination Center (IC SCC) is responsible for asset response. The Office of the Director of National Intelligence (ODNI) manages the threat and asset response for the integrated defense of the IC information environment through the IC SCC, in conjunction with IC mission partners and with support from other federal agencies, as appropriate.

Intelligence Support

Intelligence and related supporting activities play an important role to better understand the cyber incident and existing targeted diplomatic, economic, or military capabilities to respond and share threat and mitigation information with other potential affected entities or responders. Especially during a significant cyber incident, asset and threat responders should leverage intelligence support activities as necessary to build situational threat awareness; share related threat indicators and analysis of threats; identify and acknowledge gaps; and ultimately create a comprehensive picture of the incident.

State, Local, Tribal, and Territorial Government

States fusion centers involve various levels of state government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances. The fusion process should be organized and coordinated, at a minimum, on a statewide level, and each state should establish and maintain a center to facilitate the fusion process. Though the foundation of fusion centers is the law enforcement intelligence component, center leadership should evaluate their respective jurisdictions to determine what public safety and private sector entities should participate in the fusion center.

²⁷ Defense Production Act of 1950, as Amended October 2009. (50 U.S.C. App. 2061 et seq.)
<https://www.fema.gov/media-library/assets/documents/15666>

Federal Government

ODNI, through the Cyber Threat Intelligence Integration Center (CTIIC), provides intelligence support to federal agencies in response to cyber incidents. Pursuant to PPD-41, in the event of a significant cyber incident for which a Cyber UCG is convened, ODNI, through CTIIC, will serve as the lead federal agency for intelligence support and related activities. The specific responsibilities and coordinating roles for this line of effort during a significant cyber incident are detailed in the Operational Coordination During a Significant Cyber Incident section of this Plan.

In this role, CTIIC coordinates development of federal intelligence information for the other federal cybersecurity centers and federal stakeholders. This could include pursuing declassification of intelligence and/or “tear-line” reports at different classification levels as appropriate to the circumstances of the incident and overall U.S. equities. CTIIC also coordinates any intelligence collection activities that may take place as part of the incident through the National Intelligence Manager for Cyber.

Each intelligence operational center has its own organic intelligence support that aligns to its operational responsibilities. The DHS Office of Intelligence and Analysis has responsibilities under Title 6²⁸ to deliver intelligence to SLTT and private sector partners and develop intelligence from those partners for the Department and the IC. In addition, it provides intelligence support to the NCCIC’s private sector information sharing mission including gathering intelligence requirements from critical private sector companies and if the DHS National Protection and Programs Directorate concurs with the requirements can submit as formal requirements into the intelligence process.

The FBI collects and coordinates the sharing of relevant intelligence and other information between FBI domestic personnel and FBI staff assigned to Legal Attaché offices around the world; coordinates the sharing of intelligence among and between federal agencies and international intelligence and law enforcement elements; produces and shares analytical products, including those that assess threats to the homeland and inform related planning, capability development, and operational activities; and coordinates with ODNI mission and support centers that provide unique capabilities for homeland security partners.²⁹

The National Security Agency Cybersecurity Threat Operations Center (NCTOC) is the 24/7/365 NSA element that characterizes and assesses foreign cybersecurity threats. The NCTOC informs partners of current and potential malicious cyber activity through its analysis of foreign intelligence, with a focus on adversary computer network attacks, capabilities, and exploitations. Upon request, the NCTOC also provides technical assistance to U.S. Government departments and agencies.

The DoD actively characterizes and assesses foreign cybersecurity threats and informs the relevant interagency partners of current and potential malicious cyber activity. Upon request, the DoD intelligence components may provide technical assistance to U.S. Government departments and agencies; other DoD elements may provide support to civil authorities in accordance with applicable law and policy. The IC may identify classified information, indicating a potential credible cyber threat to an SLTT, critical infrastructure owner/operator, or other private sector entity. In accordance with Section 4 of Executive Order 13636, DHS and/or the FBI provide appropriate notification to the targeted entity.³⁰ Where available, declassified threat detection and mitigation information may also be provided. In circumstances where the source of threat identification, nature of the adversary, or

²⁸6 U.S.C. §124a.

²⁹ Title II of the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 118 Stat. 3638, outlines FBI intelligence authorities, as does Executive Order 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq.”

³⁰ The NCIJTF has implemented the EO 13636 4(b) tracking system, Cyber Guardian, to record the production, dissemination, and disposition of these notifications.

other factors of national security concern exist, incident response processes and procedures adhere to all guidelines and directions for handling matters of national security.

Affected Entity's Response

Entities affected by a significant cyber incident usually undertake activities to manage the effects of the cyber incident on its operations, customers, and workforce, to include complying with various legal, regulatory, or contractual obligations. When a federal agency is an affected entity, that agency has primary responsibility for engaging in a variety of efforts to manage the impact of the cyber incident. These efforts could include, but not limited to:

- Maintaining business or operational continuity;
- Mitigating potential health and safety impacts;
- Addressing adverse financial impacts;
- Protecting privacy;
- Managing liability risk;
- Complying with legal and regulatory requirements (including disclosure and notification);
- Engaging in communications with employees or other affected individuals; and
- Managing external affairs (e.g., media and congressional inquiries).

When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant SSA will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

Cyber Incidents Involving Personally Identifiable Information

As it relates to cyber incidents affecting civilian Federal Government agencies, if the facts and circumstances lead to a reasonable suspicion that the known or suspected cyber incident involves personally identifiable information, then the appropriate senior agency officials for privacy will be notified and lead any necessary personally identifiable information incident response process, as required by the Office of Management and Budget Memorandum M-07-1612, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (and its subsequent revisions), and the agency's Breach Response Plan.³¹

Core Capabilities

Core capabilities are the distinct critical elements needed to conduct the threat response, asset response, and intelligence support activities in response to a cyber incident. Core capabilities are the activities that generally must be accomplished in cyber incident response, regardless of which levels of government are involved. They provide a common vocabulary to describe the significant functions that must be developed and executed across the whole-of-Nation to ensure preparedness.

³¹ Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. May 22, 2007.
<https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>

Core capability application may be achieved with any combination of properly planned, organized, and trained personnel and deployed through various approaches such as the NIST Cybersecurity Framework or cybersecurity activities developed by the private sector. The National Preparedness Goal organizes the core capabilities into mission areas. These capabilities are aligned in Annex H: Core Capability/NIST Cybersecurity Framework/PPD-41 Crosswalk.

The capabilities are briefly described in this section and in further detail in Annex F: Core Capabilities and align with the National Preparedness Goal core capabilities.³² While Annex F is not an exhaustive list of capabilities, it provides a description of the capabilities that should be developed and utilized for particular needs, and roles, responsibilities, and authorities for the nature and scope of the cyber incident. All levels of government, private and non-profit sector organizations, and critical infrastructure owners and operators should assess their particular risks to identify their core capability requirements. Annex I describes additional resources that can be leveraged by both the private and public sector. Those resources can also serve as a starting point for understanding cyber incident response, vulnerability updates, data breach information, risk management, and organizations.

Responding to a cyber incident, like incident response for all other threats and hazards, is a shared responsibility. The whole-of-Nation must work together to ensure the United States is optimally prepared for cyber incidents; recognizing that not every network/system faces the same risks. By engaging the whole-of-Nation to build and deliver the cyber response core capabilities, the Nation is better prepared to respond to any threat or hazard, assist in restoring basic services and community functionality, and facilitate the integration of recovery activities.

Access Control and Identity Verification

Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems, which is also referred to as Authentication and Authorization. This capability relies on the implementation and maintenance of protocols to verify identity and authorize, grant, or deny access to specific IT systems and networks.

Cybersecurity

Description: Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as information security, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts.

Forensics and Attribution

Description: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.

Forensics: Forensics is the term for discovering and identifying information relevant to an investigation through both scientific and intelligence-based acumen. In the context of a cyber incident, forensics refers to a number of technical disciplines related to the duplication, extraction, and analysis of data to uncover artifacts relevant to identifying malicious cyber activity. Forensics includes several sub-disciplines, including host-based forensics, network and packet data forensics,

³² <https://www.fema.gov/core-capabilities>

memory analysis, data correlation, and malware analysis.

During the response to a significant cyber incident, government agencies and private sector partners frequently conduct simultaneous analysis and share analytical results with each other to create a common understanding regarding the malicious cyber activity and how to defend against these or similar activity. In the days following an incident, a number of different threat, asset, and business response organizations may also engage in simultaneous forensic analysis. Although these lines of effort may appear to be duplicative, findings from these efforts could vary depending on the entities' varied access to particularized datasets or holdings.

Attribution: Attribution identifies an adversary linked to a particular incident. It is the culmination of the review of evidence and intelligence gathered during an incident which results in an assessment that identifies individuals or organizations which likely played a role in the cyber incident.

Attribution occurs over the lifecycle of an investigation and may not be known at the onset of a cyber incident response. Although the development of attribution for a significant cyber incident is one of the primary functions of lead federal response agencies, other government and private sector entities have a significant role to play in determining attribution.

An assessment regarding attribution for an incident is not only important for government agencies conducting criminal or national security investigations; it could also be significant to an affected entity as it considers whether to pursue additional legal or civil action against threat actors.

This core capability also includes unique and technical activities that support computer network and asset analysis during an incident. These supporting activities contribute to awareness of a comprehensive picture, which ultimately helps reduce the impact of a current incident and prevent future cyber incidents from spreading across the network.

Infrastructure Systems

Description: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity. Critical infrastructure and cyber networks are interdependent. In a response to a cyber incident, this capability focuses on stabilizing the infrastructure assets and entities, repairing damaged assets, regaining control of remote assets, and assessing potential risks to the critical infrastructure sector at large.

Intelligence and Information Sharing

Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.

In the context of a cyber incident, this capability involves the effective implementation of the intelligence cycle and other information collection and sharing processes by federal and SLTT entities, the private sector, and international partners to develop situational awareness of potential cyber threats to the United States.

Interdiction and Disruption

Description: Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity. In the context of a cyber incident, these threats include people, software, hardware, or

activities that pose a threat to the Nation's cyber networks and infrastructure. This includes those interdiction and disruption activities that may be undertaken in response to specific, actionable intelligence of a cyber threat. Interdiction and disruption may include the targeting of persons, programs, or equipment or machines to stop or thwart threat activities and employing technical and other means to prevent malicious cyber activities. Interdiction and disruption capabilities help thwart emerging or developing cyber threats and neutralize operations. These capabilities should be utilized in a manner that preserves evidence and the Government's ability to prosecute those who violate the law.

Logistics and Supply Chain Management

Description: Facilitate and assist with delivery of essential commodities, equipment, and services in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.

In the context of a cyber incident, this capability focuses on providing the logistical or operational support to achieve cyber incident response priorities established by leadership through identifying, prioritizing, and coordinating immediate response resource requirements.

Operational Communications

Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.

In the context of a cyber incident, this capability includes identifying federal support organizations, capabilities, and teams with internal interoperable voice, video, and data systems and networks essential for effective cyber incident response operations. In a cyber incident, this capability focuses on the timely, dynamic, and reliable movement and processing of incident information in a form that meets the needs of decision makers at all levels of government and authorized participating private sector partner organizations.

Operational Coordination

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities. This is the capability to conduct actions and activities that enable decision makers across the whole-of-Nation to determine appropriate courses of action and to provide oversight for complex operations, to achieve unity of effort and effective outcomes. Operational coordination, in accordance with the principles of the NIMS and the Incident Command System, coordinates the threat response, asset response, and intelligence support activities in the face of a cyber threat or in response to an act of terrorism committed in the homeland. Unity of message is included within the guiding principles. Further information is available in Annex D: Reporting Cyber Incidents to the Federal Government.

In the context of a cyber incident, this core capability includes efforts to coordinate activities across and among all levels of government and with private sector partners. This capability involves national operations centers, as well as on-scene response activities that manage and contribute to multi-agency efforts.

Planning

Description: Conduct a systematic process engaging the whole-of-Nation, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined

objectives.

In the context of a cyber incident, planning includes both deliberate planning and incident action planning. Deliberate planning involves developing strategic, operational, and tactical plans to prevent, protect against, mitigate the effects of, respond to, and recover from a cyber incident. Incident action planning occurs in a time-constrained environment to develop or rapidly adapt operational and tactical plans in response to an imminent or ongoing cyber incident.

Public Information and Warning

Description: Deliver coordinated, prompt, reliable, and actionable information to the whole-of-Nation and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threats or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.³³

In the context of a significant cyber incident, this capability uses effective and accessible indications and warning systems to communicate significant cyber threats to involved or potentially involved operators, security officials, and the public (including alerts, detection capabilities, and other necessary and appropriate assets).

Screening, Search, and Detection

Description: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.

In the context of a cyber incident, this capability includes the measures which may be taken in response to actionable intelligence that indicates potential targets or types of malicious cyber activity, or the threat actors planning such activity. Measures may also be taken to verify or characterize a cyber threat that has already been located. Screening relative to a cyber incident may include monitoring the status of the network, assets, sensors, and other technologies that provide information on the security posture that may determine further action as necessary.

Situational Assessment

Description: Provide all decision makers with timely, decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.

In the context of a cyber incident, this capability focuses on rapidly processing and communicating large quantities of information from across the broader community, from the field level to the national level, to provide all decision makers with the most current and accurate information possible.

Threats and Hazards Identification

Description: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude of those threats; and incorporate this into analysis and planning processes

³³ The President of the United States has directed the Secretary of Homeland Security and the Attorney General to coordinate with each other to execute key responsibilities that provide public information and warning to the Nation regarding threats and incidents.

so as to clearly understand the needs of an entity.

In the context of a cyber incident, this capability involves the continual process of collecting timely and accurate data on cyber threats, including accounting for the future impacts of technology advancements, to meet the needs of analysts and decision makers. Effective Threats and Hazards Identification for a cyber incident is supported by standardized data sets, platforms, methodologies, terminologies, metrics, and reporting to unify levels of effort across all layers of government and the private sector, reducing redundancies.

Coordinating Structures and Integration

Successfully managing cyber incidents requires a whole-of-Nation approach (as described in the introduction of this document) that facilitates coordination among all stakeholders, including the private sector, SLTT governments, federal agencies, and international partners. Governing entities organize that coordination through established structures that promote unity of effort during incident response.

Coordinating structures provide a mechanism for representatives of entities that are affected by or are responsible for responding to a cyber incident to coordinate and facilitate response activities. These coordination and response activities may include preparedness activities, the delivery of capabilities, development operational plans, coordination of response personnel and activities, the crafting of unified public messaging and alerts, and weighing the technical, operational, political, and policy implications of varying courses of action.

While existing policies and coordinating structures can handle the vast majority of cyber incidents, significant cyber incidents may require a unique approach to coordinating the whole-of-Nation response. Pursuant to PPD-41, the U.S. Government will establish a Cyber UCG as the primary method for coordinating between and among federal agencies responding to a significant cyber incident, as well as for integrating SLTT governments and private sector partners into incident response efforts as appropriate for the specific incident. Other coordinating structures should be prepared to integrate and interoperate with a Cyber UCG, if one is established.

This section describes the major coordination structures in place across stakeholder communities that can be leveraged for response to cyber incidents requiring external coordination. Specifically, it describes how these structures will be leveraged, and additional structures incorporated, to provide operational coordination in response to significant cyber incidents.

Coordinating Structures

Stakeholders can utilize a variety of existing coordinating structures during any cyber incident to facilitate information sharing, coordinate response activities, access technical assistance and other resources, provide policy coordination and direction, and enable effective response. Most cyber incidents that occur on a daily basis are considered routine, and their responses are handled internally by the affected entity. As such, affected entities may choose to combine any of the coordinating structures below as deemed necessary to address the unique nature of the incident and specific organizational or sector needs. For significant cyber incidents, or cyber incidents that have implications for national security or public health and safety, PPD-41 establishes lead federal agencies and a coordinating structures framework with operational response planning and activities coordinated through a Cyber UCG.

Private Sector

For many years, the private sector has successfully engaged in coordination efforts between and across industry and government around detection, prevention, mitigation, and response to cyber

incidents through information sharing, analysis, and collaboration. Each of the 16 critical infrastructure sectors and sub-sectors designated under PPD-21: *Critical Infrastructure Security and Resilience*,³⁴ has a self-organized and self-governed Sector Coordinating Council (SCC). SCC members include critical infrastructure owners and operators, industry trade associations, and others across the private sector. SCCs provide a forum for members to engage with others across their sector, companion Government Coordinating Councils (GCCs), and SSAs to collaboratively address the full range of sector-specific and cross-sector critical infrastructure security and resilience policy and strategy efforts.

In addition, the private sector critical infrastructure community has developed its own coordination efforts through established ISACs. ISACs are based in and organized and governed by the private sector (with the exception of the MS-ISAC discussed later), with operational capabilities that support the public-private partnership around critical infrastructure protection and cybersecurity every day. The National Council of ISACs routinely facilitates cross-sector coordination to further productive engagement across the private sector and with government at the federal, state, and local levels.

As mentioned earlier, in accordance with policy established by Executive Order 13691, DHS is facilitating efforts to identify procedures to create and accredit ISAOs³⁵ to allow groups of stakeholders to create information sharing groups based on affinity among members (e.g., geography, industry or community segment, or threat exposure) that could provide a more formalized structure for information sharing and the provision of technical assistance. Some organizations, including those that are well established and delivering value every day, may be recognized as an ISAO and or ISAC, or as a member of more than one, concurrently. ISACs predate and are a subset of ISAOs.

State, Local, Tribal, and Territorial Governments

These levels of government also have a variety of coordination structures available to them for cyber incident response. These structures support information sharing, incident response, operational coordination, and collaboration on policy initiatives among participating governments.

As with private sector organizations, SLTT governments can be members of ISACs, ISAOs, or other information sharing organizations. They could also be members of the SLTT GCC at the national policy coordination level. For incidents on SLTT government networks MS-ISAC provides information sharing and technical assistance to its members and has established relationships with the Federal Government. As owners and operators of critical infrastructure and key resources, certain SLTT government agencies could also be members of sector-specific ISACs and may also develop unique structures, tailored to their jurisdiction's needs, to provide coordination and direction to response officials during a cyber incident. Many also collaborate with one another through selected cyber information sharing groups or organizations such as the National Association of State Chief Information Officers or the National Governors' Association.

While many SLTT governments are developing and utilizing operational coordination structures for cyber incident response, they have not all adopted a standard approach. Some may designate their state or major urban area fusion center as the primary contact and information sharing hub for cyber incident coordination while others could leverage their respective emergency or security operations center. For cyber incidents with physical effects, or that have consequences that must be managed in collaboration with other emergency management agencies (e.g., fire departments, public health agencies, human services offices), emergency operations centers will also likely provide important

³⁴ <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

³⁵ www.isao.org

information sharing and incident management functions. At the state/territory level, emergency operations centers often coordinate resource requests with federal agencies, including FEMA and DoD, and provide operational coordination with the National Guard. The SLTT community are encouraged to provide cross-functional training in cybersecurity for the employees of their emergency operations center. As appropriate, cyber incident responders should also receive emergency response and emergency operations center training.

Federal Government

The Federal Government organizes coordinating structures into three categories for cyber incident response:

- National policy level coordination through the Cyber Response Group (CRG),³⁶
- Operational coordination through Federal Cybersecurity Centers and federal agencies, and
- Sector coordination through the SSAs and GCCs.

To coordinate policy at the National level, PPD-41 assigns the Assistant to the President for Homeland Security and Counterterrorism the responsibility to convene and chair the CRG to coordinate development and implementation of Federal Government policy and strategy with respect to significant cyber incidents affecting the Nation or its interests abroad. The CRG will coordinate the development and implementation of U.S. Government policy and strategy for responding to significant cyber incidents. Federal departments and agencies, including relevant cybersecurity centers, are invited to participate in the CRG, as appropriate, based on their respective roles, responsibilities, and expertise or in the circumstances of a given incident or grouping of incidents. Federal agencies, including SSAs that regularly participate in the CRG must establish and implement enhanced coordination procedures to manage significant cyber incidents that exceed their standing response capacities.

The Federal Government has established seven cybersecurity centers, with missions that include executing cyber operations, enhancing information sharing, maintaining situational awareness, and serving as conduits between public and private sector entities. Any or all of these centers should coordinate with federal entities and provide support to cyber incident response to the extent circumstances dictate and authorities permit. Pursuant to PPD-41, three of these centers coordinate significant cyber incident response activities within a Cyber UCG: the NCCIC, the NCIJTF, and CTIIC.

The Federal Government has also designated a number of SSAs to lead their sector GCCs, which are governmental counterparts to SCCs. SSAs are designated for each of the 16 critical infrastructure sectors designated under PPD-21. SSAs leverage their particular knowledge and expertise to fulfill a number of information sharing, coordination, incident response, and technical assistance responsibilities to their assigned critical infrastructure sector(s), as detailed in PPD-21 and the NIPP. GCCs include other government agencies with authorities and expertise in a given sector; robust engagement across GCC participants will enable interagency and interjurisdictional coordination by including broader participation from federal and SLTT governments, as appropriate to the needs of each sector.

³⁶ More information on the Cyber Response Group can be found within PPD-41: *U.S. Cyber Incident Coordination*. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident-Annex-for-Presidential-Policy-Directive-41--United-States-Cyber-Incident-Coordination>. <https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident>.

International

International information sharing takes place through a variety of mechanisms in both the public and private sectors. Many organizations have information sharing relationships that extend to international partner companies and governments. International operational coordination can occur through relationships that federal departments and agencies have with their foreign counterparts and with international organizations, through formal diplomatic channels managed by DOS and through the relationships that private firms have internally, with other private sector entities, with national governments, and with international organizations.

Many federal agencies and cybersecurity centers have relationships with counterparts in foreign nations and routinely share information and collaborate, both during steady state and cyber incidents. Federal law enforcement agencies also maintain information sharing channels with foreign counterparts and the International Criminal Police Organization (INTERPOL) to facilitate international investigations. The FBI, through its Legal Attaché program, has designated Cyber liaison attaches stationed in U.S. Embassies. DHS/ICE HSI has broad legal authority to enforce a diverse array of federal statutes and uses this authority to investigate all types of cross-border criminal activity. The U.S. Secret Service maximizes partnerships with international law enforcement counterparts through overseas field offices and by forward deploying the Electronic Crimes Special Agent Program to international working groups. The NCCIC collaborates with international CSIRT partners to obtain situational awareness and determine priorities for protection and response. Organizations such as the DOS Overseas Security Advisory Council, for example, coordinates information sharing and collaborative security activity and analysis for U.S. private sector interests abroad through an industry representative council structure and established channels at U.S. embassies and other diplomatic posts. Additionally, some ISACs have chosen to open membership to firms and organizations located in friendly foreign nations, with safeguards in place to preserve confidentiality of information restricted to U.S. participants.

Given existing relationships and the overlapping policy and operational issues that may arise during a significant cyber incident, it is important to note that international coordination will likely occur through multiple channels concurrently.

Operational Coordination During a Significant Cyber Incident

Cyber incidents affect domestic stakeholders on an ongoing basis. The vast majority of these incidents pose no demonstrable risk to the U.S. national security interests, foreign relations, economy, public confidence, civil liberties, or public health and safety and thus do not rise to the designation of a significant cyber incident as defined by PPD-41 and the accompanying Cyber Incident Severity Schema in Annex B. Such cyber incidents are resolved either by the affected entity alone or with routine levels of support from, and in coordination with, other private sector stakeholders and/or from SLTT, federal, or international government agencies. In the event of a significant cyber incident, the Federal Government may form a Cyber UCG as the primary method for coordinating between and among federal agencies responding to a significant cyber incident and for integrating private sector partners into incident response efforts as appropriate.

Determination of Incident Severity

The Federal Government adopted the Cyber Incident Severity Schema in Annex B as a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments and agencies when determining the severity of a cyber incident. Cyber incidents rated a “3” or greater will equate to a significant cyber incident. Federal Government departments and agencies shall leverage the Cyber Incident Severity Schema when assessing the severity level and the potential impact of cyber incidents to ensure common terminology, appropriate information sharing, and

proper management to effectively address an incident. As referenced earlier, Annex C compares the Cyber Incident Severity Schema and Activation Level of the National Response Coordination Center to demonstrate alignment cyber and physical incidents. When assessing the severity of a potentially significant incident, the federal cybersecurity centers that serve as lead federal agencies under PPD-41 (the NCCIC, NCIJTF, and CTIIC) will consult to make a joint assessment of severity.

Our Nation's critical infrastructure sectors are composed of public and private owners and operators, both of which provide vital services and possess unique expertise and experience that the Federal Government and Nation rely heavily upon. Therefore, when determining incident severity, DHS, through the NCCIC and the SSAs of sectors affected or likely to be affected, may consult with sector leadership and private sector owners and operators through organizations such as the sector ISAC(s), SCC, GCC, the National Council of ISACs, MS-ISAC, and/or the Partnership for Critical Infrastructure Security if the incident affects or is likely to affect a non-federal entity in one or more of the critical infrastructure sectors. The private sector assessment would inform the NCCIC severity rating of a cyber incident.

With the majority of critical infrastructure owned and operated by the private sector, it is more than likely that the Federal Government may learn of a potential significant cyber incident through voluntary self-reporting and information sharing from the affected entity or a sector coordinating mechanism. Non-federal entities are also encouraged to utilize the Cyber Incident Severity Schema and/or the NCCIC Cyber Incident Scoring System³⁷ to help organizations provide a repeatable and consistent mechanism for estimating the risk of an incident.

Additionally, when a significant cyber incident affects a private sector stakeholder, SLTT government, or international counterpart, they have several options for voluntarily sharing the issue with federal authorities including:

- The NCCIC, FBI, or NCIJTF;
- Applicable SSA(s) or regulators; or
- The local field office of federal law enforcement agencies, including the FBI, U.S. Secret Service, U.S. ICE/HSI, or relevant Military Criminal Investigative Organizations if defense related.

Points of contact for reporting incidents to Federal Government entities are provided in Annex D: Reporting Cyber Incidents to the Federal Government. In addition to voluntary reporting, affected entities that have mandatory reporting requirements according to law, regulation, or contract must continue to comply with such obligations.

The federal agency that receives the report will coordinate with other federal agencies in responding to the incident, including determining whether or not to establish a Cyber UCG to coordinate the response to the significant cyber incident. As a part of this determination, stakeholders can provide information and assessments to federal agencies regarding their view of the severity of the incident for their entity and for their sector. Federal agencies will leverage these assessments and engage with the affected entity for discussion as part of the decision process. As appropriate, the Federal Government also engages with relevant private sector organizations, ISACs, ISAOs, SCCs, SLTT governments, and/or international stakeholders for consultation about the severity and scope of the incident.

³⁷ National Cyber Incident Scoring System. <https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System>.

Enhanced Coordination Procedures

Per PPD-41, each federal agency that regularly participates in the CRG, including SSAs, ensures that it has the standing capacity to execute its role in cyber incident response. Agencies establish enhanced coordination procedures to prepare for significant cyber incidents that exceed its standing capacity. These procedures require dedicated leadership, supporting personnel, available facilities (physical and communications), and internal processes enabling it to manage a significant cyber incident under demands that would exceed its capacity to coordinate under normal operating conditions.

Enhanced coordination procedures help to:

- Identify the appropriate pathways for communicating with other federal agencies during a significant cyber incident, including the relevant agency points-of-contact, and for notifying the CRG that enhanced coordination procedures were activated or initiated;
- Highlight internal communications and decision-making processes that are consistent with effective incident coordination; and
- Outline processes for maintaining these procedures.

In addition, each federal agency's enhanced coordination procedures identify the agency's processes and existing capabilities to coordinate cyber incident response activities in a manner consistent with PPD-41. Government and private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information. PPD-41 also directs SSAs to develop or update sector-specific procedures, as needed and in consultation with the sector(s), for enhanced coordination to support response to a significant cyber incident, consistent with this directive. These sector-focused procedures serve as a key mechanism for integrating government and private sector response processes, including processes for accounting for and responding to the business impacts of significant incidents.

Cyber UCG

A Cyber UCG, per PPD-41, serves as the primary national operational coordination mechanism between and among federal agencies responsible for identifying and developing operational response plans and activities during a significant cyber incident, as well as for integrating private sector partners and the SLTT communities into incident response efforts, as appropriate.

Authorities

The Cyber UCG works to establish shared objectives for threat response, asset response, and intelligence support to guide cyber incident response and recovery efforts in the short to mid-term. PPD-41 establishes the Cyber UCG and frames this concept of operations. PPD-41 does not alter, supersede, or limit the authorities of federal agencies to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives. Instead, PPD-41 complements and builds upon PPD-8 on National Preparedness by integrating cyber and traditional preparedness efforts to manage incidents that include both cyber and physical effects. It also leverages the SSA construct and assignments of PPD-21 on Critical Infrastructure Security and Resilience. The Cyber UCG bolsters a unity of effort and does not alter agency authorities or leadership, oversight, or command responsibilities, unless mutually agreed upon between the relevant agency heads and consistent with applicable legal authorities, including the Economy Act of 1932.

Cyber UCG Formation

A Cyber UCG will be formed and activated only in the event of a significant cyber incident and will be incident specific. Cyber UCG will be formed by any of the following processes:

- At the direction of the National Security Council Principals Committee (Secretary level), Deputies Committee (Deputy Security level), or the CRG;
- When two or more federal agencies that generally participate in the CRG, including relevant SSAs, request its formation based on their assessment of the cyber incident against the severity schema; and or
- When a significant cyber incident affects critical infrastructure owners and operators identified by the Secretary of Homeland Security for which a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security

A Cyber UCG will dissolve when enhanced coordination procedures for threat and asset response are no longer required or the authorities, capabilities, or resources of more than one federal agency are no longer required to manage the remaining facets of the federal response to an incident.

Cyber UCG Responsibilities

Per PPD-41, a Cyber UCG conducts the following activities to promote unity of effort in response to a significant cyber incident:

- Coordinates the cyber incident response in a manner consistent with the principles described in the Section III of PPD-41 Annex;
- Ensures all appropriate federal agencies, including SSAs, are incorporated into the incident response;
- Coordinates the development and execution of response and recovery tasks, priorities, and planning efforts, including international and cross-sector outreach, necessary to respond appropriately to the incident and to speed recovery;
- Facilitates the rapid and appropriate sharing of information and intelligence among Cyber UCG participants on the incident response and recovery activities;
- Coordinates consistent, accurate, and appropriate communications regarding the incident to affected parties and stakeholders (and those who could be affected), including the public as appropriate; and
- For incidents that include cyber and physical effects, forms a combined UCG with the lead federal agency or with any UCG established to manage the physical effects of the incident under the NRF developed pursuant to PPD-8: *National Preparedness*,³⁸ or other applicable presidential policy directives.

The Cyber UCG will promptly coordinate with DOJ, general counsel from DHS, regulators, and other relevant federal agencies' attorneys about pertinent legal issues as they are identified to quickly consider and coordinate them with appropriate nongovernmental entities, as necessary.

³⁸ PPD-8, *National Preparedness*, March 30, 2011. <https://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf>.

Cyber UCG Participation

Per PPD-41, when a Cyber UCG is established, the Federal Government establishes three lead agencies to effectively respond to significant cyber incidents:

- DHS is the lead agency for **asset response** during a significant cyber incident, acting through the NCCIC. The NCCIC includes representation from the private sector, SLTT, and numerous federal agencies. It is a focal point for sharing cybersecurity information, information about risks and incidents, analysis, and warnings among federal and non-federal entities.
- DOJ is the lead agency for **threat response** during a significant cyber incident, acting through the FBI and the NCIJTF. Consisting of over 20 partner agencies from across law enforcement, the IC, and the DoD, the NCIJTF serves as a multi-agency focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations.
- ODNI is the lead coordinator for **intelligence support** during a significant cyber incident, acting through the CTIIC. CTIIC provides situational awareness, sharing of relevant intelligence information, integrated analysis of threat trends, events, and support to interagency efforts to develop options to degrade or mitigate adversary threat capabilities. CTIIC also coordinates any intelligence collection activities that may take place as part of the incident, including identification of intelligence gaps, through the National Intelligence Manager, Cyber. Drawing upon the resources and capabilities across the Federal Government, the lead federal agencies are responsible for:
 - Coordinating any multi-agency threat or asset response activities to provide unity of effort, to include coordinating with any agency providing support to the incident, to include SSAs in recognition of their unique expertise;
 - Ensuring that their respective lines of effort are coordinated with other Cyber UCG participants and affected entities, as appropriate;
 - Identifying and recommending to the CRG, if elevation is required, any additional Federal Government resources or actions necessary to appropriately respond to and recover from the incident; and
 - Coordinating with affected entities on various aspects of threat, asset, and affected entity response activities through a Cyber UCG, as appropriate.

In addition to the lead federal agencies, a Cyber UCG will also include SSAs, if the cyber incident affects or is likely to affect sectors they represent as well as other federal cybersecurity centers as deemed necessary per the specific significant cyber incident. All federal agencies responding to the significant cyber incident will participate in, and coordinate their response activities with, a Cyber UCG.

SLTT government will be asked to participate in a Cyber UCG when the government entity owns or operates critical infrastructure that is or may be affected by that particular significant cyber incident. Otherwise, the Cyber UCG will use existing collaboration and information sharing mechanisms to provide regular updates to SLTT partners.

Like government participation, private sector involvement in a Cyber UCG will be limited to organizations with significant responsibility, jurisdiction, capability, or authority for response for that specific incident, which may not always include all organizations contributing resources to the response. Private Sector Cyber UCG participation will be voluntary and participants should be from organizations which can determine the incident priorities for each operational period and approve an Incident Action Plan, to include commitment of their organizations' resources to support execution of the Incident Action Plan. Per the Guiding Principles in PPD-41, out of respect for an affected

entities' privacy and sensitive private sector information, the Federal Government will coordinate with the affected entity on the approach of wider incident dissemination for that incident. Cyber UCG participants will be expanded or contracted as the situation changes during that particular incident response.

Depending on the nature and extent of the incident, a Cyber UCG might also incorporate specific ICT³⁹ companies, also known as ICT enablers, to directly assist on that specific incident response. ICT enablers are companies whose functions and capabilities are the foundations of the global cyber ecosystem. As such, it is these ICT enablers who are often best positioned to share information, ensure engagement of key players across the Internet and ICT realms, and assist with large-scale response efforts during a significant cyber incident.

Additionally, the Cyber UCG will continue to use several pre-existing and well-established coordinating structures, such as SCCs, ISACs and routine operational calls, for information sharing to ensure appropriate and timely sharing of actionable intelligence. As the operational arm for many sectors, ISACs especially can assist in their specific sector and across sectors impact assessment as the specific incident allows. Additional organizations may be engaged in response as participants in a Cyber UCG staff or as liaising organizations working in cooperation with the incident management team under separate leadership structures. Such organizations would generally have awareness of and opportunities to provide input to the Incident Action Plan, but would not be responsible for its contents or execution.

Regardless of specific participant composition, a Cyber UCG shall operate in a manner that is consistent with the need to protect intelligence and law enforcement sources, methods, operations, and investigations, the privacy of individuals, and sensitive and protected private sector information.

Information Sharing During Cyber Incident Response

Cyber UCGs share cyber threat information developed during incident response with other stakeholders as quickly, openly, and regularly as possible, to ensure protective measures can be applied with all applicable stakeholders. This sharing may at times be constrained by law, regulation, interests of the affected entity, classification or security requirements, or other operational considerations. However, participants will strive for unity of message when sharing with stakeholders and the public. Existing cyber threat information sharing channels will be used to disseminate such information where feasible.

In some cases, depending on how a Cyber UCG's participants have decided to staff a particular incident, this sharing could also take place via a Public Information Officer designated by the Cyber UCG or via a Joint Information Center staffed by representatives of responding organizations. In some cases, ad hoc information sharing mechanisms are required to provide effective situational awareness to interested or affected stakeholders. In all cases, Cyber UCGs protect the privacy of individuals and sensitive private sector information, as appropriate.

Conclusion

America's efforts to strengthen the security and resilience of networked technologies are never finished. To achieve this security and resilience, the public-private partnership is integral to collectively identifying priorities, articulating clear goals, mitigating risk, and adapting and evolving based on feedback and the changing environment. The Federal Government, SLTT governments, and

³⁹ The President's National Security Telecommunications Advisory Committee's Information Technology Mobilization Scoping Report. May 21, 2014. <https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf>

the Private and International partners remain resolute in its commitment to safeguard networks, systems and applications against the greatest cyber risks it faces, now and for decades to come.

The DHS Office of Cybersecurity and Communications will coordinate and oversee reviews and maintenance of the NCIRP in coordination with the DOJ, ODNI, and SSAs. The revision process includes developing or updating any documents necessary to carry out capabilities. Significant updates to the Plan will be vetted through a public-private senior-level review process. This Plan will be reviewed in order to accomplish the following:

- Assess and update information on the core capabilities in support of cyber and cyber-physical incident response goals and objectives.
- Ensure that it adequately reflects the organization of responsible entities.
- Ensure that it is compatible with doctrine and practices for the protection, prevention, mitigation, response, and recovery mission areas of the National Preparedness Goal.
- Update processes based on changes in the national threat/hazard environment.
- Incorporate lessons learned and effective practices from day-to-day operations, exercises, and actual incidents and alerts.
- Adapt to opportunities and challenges that arise as technology evolves and changes.
- Reflect progress in the Nation's cyber incident response mission activities, the need to execute new laws, executive orders, and Presidential directives, as well as strategic changes to national priorities and guidance, critical tasks, or national capabilities.

Additions or updates to the NCIRP annexes may occur independently from reviews of the base document based on lessons learned from immediate statute or law changes, cyber exercises or real world incidents.

Annex A: Authorities and Statutes

The authorities listed below provide the legal basis for Federal Government threat response, asset response, and intelligence support activities. Other laws and regulations place additional requirements on certain critical infrastructure sectors.

This list is not exhaustive, but it can be leveraged as a foundational resource.

- Communications Act of 1934, Section 706 (Public Law [PL] 73-416)
- Cybersecurity Act of 2015 (PL 114 – 113)
- Defense Production Act of 1950 (PL 81-744), as amended
- Executive Order (EO) 12333: *United States Intelligence Activities*, as amended
- EO 12382: *President’s National Security Telecommunications Advisory Committee, as amended*
- EO 12829: *National Industrial Security Program*, as amended
- EO 12968: *Access to Classified Information*, as amended
- EO 13549: *Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities*
- EO 13618: *Assignment of National Security and Emergency Preparedness Communications Functions*
- EO 13636: *Improving Critical Infrastructure Cybersecurity*
- EO 13691: *Promoting Private Sector Cybersecurity Information Sharing*
- Federal Information Security Modernization Act of 2014 (PL 113-283)
- Homeland Security Act of 2002 (as amended through Public Law 112-265)
- Homeland Security Presidential Directive (HSPD)-5: *Management of Domestic Incidents*
- Intelligence Authorization Act for Fiscal Year 2004 (PL 108-177)
- Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458)
- National Cybersecurity Protection Act of 2014 (PL 113-282)
- National Infrastructure Protection Plan of 2013, *Partnering for Critical Infrastructure Security and Resilience*
- National Security Act of 1947 (PL 80-253), as amended
- National Security Directive 42: *National Policy for the Security of National Security Telecommunications and Information Systems*
- National Security Presidential Directive-54/ HSPD-23: *Cybersecurity Policy*
- Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*
- Presidential Policy Directive (PPD)-8: *National Preparedness*
- PPD-21: *Critical Infrastructure Security and Resilience*
- PPD-25: *U.S. Policy on Reforming Multilateral Peace Operations*
- PPD-40: *National Continuity Policy*

- PPD-41: *U.S. Cyber Incident Coordination Policy* and its accompanying Annex
- U.S. Code (USC) Title 6 – Domestic Security
- USC Title 10 – Armed Forces
- USC Title 18 – Crimes and Criminal Procedure
- USC Title 32 – National Guard
- USC Title 47 - Telecommunications
- USC Title 50 – War and National Defense

Annex B: Cyber Incident Severity Schema

Per Presidential Policy Directive (PPD)-41⁴⁰, the U.S. federal cybersecurity centers, in coordination with departments and agencies with a cybersecurity or cyber operations mission, adopted a common schema for describing the severity of cyber incidents affecting the homeland, U.S. capabilities, or U.S. interests. The schema establishes a common framework to evaluate and assess cyber incidents to ensure that all departments and agencies have a common view of the:

- Severity of a given incident;
- Urgency required for responding to a given incident;
- Seniority level necessary for coordinating response efforts; and
- Level of investment required for response efforts.

Figure 1 below depicts several key elements of the schema.

General Definition		Observed Actions	Intended Consequence ¹
Level 5 <i>Emergency</i> (Black)	<i>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.</i>	Effect	Cause physical consequence
Level 4 <i>Severe</i> (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.</i>		Damage computer and networking hardware
Level 3 <i>High</i> (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Presence	Corrupt or destroy data
Level 2 <i>Medium</i> (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>		Deny availability to a key system or service
Level 1 <i>Low</i> (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Engagement	Steal sensitive information
Level 0 <i>Baseline</i> (White)	Unsubstantiated or inconsequential event.	Preparation	Commit a financial crime Nuisance DoS or defacement

Figure 1: Elements of the Cyber Incident Severity Schema

⁴⁰ <https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf>

Annex C: Cyber Incident Severity Schema/ National Response Coordination Center Activation Crosswalk

When incidents impact the cyber and/or physical environment(s), certain decisions and activities require coordination in order to respond in the most appropriate manner. The graphic below compares the Cyber Incident Severity Schema released in Presidential Policy Directive 41: United States Cyber Incident Coordination and the Department of Homeland Security National Response Coordination Center Activation Scale when comparing response levels for cyber and physical incidents.

Description	Disaster Level	Cyber Incident Severity	Description	Observed Actions
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 <i>Emergency</i>	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.	Effect
Requires elevated coordination among federal and SLTT governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.	Level 2	Level 4 <i>Severe</i>	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Presence
		Level 3 <i>High</i>	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Requires coordination among federal and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 <i>Medium</i>	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement
		Level 1 <i>Low</i>	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
No event or incident anticipated. This includes routine watch and warning activities.	Level 4	Level 0	Unsubstantiated or inconsequential event.	Steady State

Annex D: Reporting Cyber Incidents to the Federal Government¹

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber incidents that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from Federal Government agencies, which are prepared to investigate the incident, help mitigate its consequences, and to help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims.

In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This Appendix explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government. A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- Result in a significant loss of data, system availability, or control of systems;
- Impact a large number of victims;
- Indicate unauthorized access to, or malicious software present on, critical information technology systems;
- Affect critical infrastructure or core government functions; or
- Impact national security, economic security, or public health and safety.

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal executive Branch civilian agencies to notify and consult with US-CERT regarding information security incidents involving their information and information systems, whether managed by a federal agency, contractor, or other source.

What to Report. A cyber incident may be reported at various stages, even when complete information is not available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

¹ This document was created in conjunction with Presidential Policy Directive 41 to provide the public with a unified federal message explaining how and when to report cyber incidents for purposes of obtaining assistance from the Federal Government. It does not address mandatory reporting pursuant to law, regulation, or contract. Such required reporting should continue to occur through designated federal points of contact using existing procedures.

How to Report Cyber Incidents to the Federal Government. Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, or any of the federal agencies listed in Table 1 below. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders to respond to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation, in addition to voluntarily reporting the incident to an appropriate federal point of contact. Federal agencies also collaborates with state, local, territorial and tribal government organizations as appropriate given the nature of the cyber incident.

Types of Federal Incident Response. Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: threat response and asset response:

- **Threat response** includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity.
- **Asset response** includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community and mitigating potential privacy risks to affected individuals.

Irrespective of the type of incident or its corresponding response, federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Table 1: Key Federal Points of Contact

Threat Response	Asset Response
<p>Federal Bureau of Investigation (FBI): FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field Internet Crime Complaint Center (IC3): http://www.ic3.gov</p> <ul style="list-style-type: none"> ▪ Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces. ▪ Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties. 	<p>National Cybersecurity and Communications Integration Center (NCCIC) (888) 282-0870 or NCCIC@hq.dhs.gov</p> <p>United States Computer Emergency Readiness Team: http://www.us-cert.gov</p> <ul style="list-style-type: none"> ▪ Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.
<p>National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center: cywatch@ic.fbi.gov or (855) 292-3937</p> <ul style="list-style-type: none"> ▪ Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government. 	

Threat Response	Asset Response
<p>United States Secret Service (USSS) Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices</p> <ul style="list-style-type: none"> ▪ Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information. 	
<p>United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI) HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or www.ice.gov/webform/hsi-tip-form HSI Field Offices: https://www.ice.gov/contact/hsi HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes</p> <ul style="list-style-type: none"> ▪ Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering. 	

If there is an immediate threat to public health or safety, the public should always call 911.

Annex E: Roles of Federal Cybersecurity Centers

The Federal Government has established a number of cybersecurity centers associated with various departments and agencies to execute operational missions, enhance information sharing, maintain situational awareness of cyber incidents, and serve as conduits between public-and private-sector stakeholder entities. In support of the Federal Government's coordinating structures on cyber incident management, a Cyber Unified Coordination Group⁴¹ may elect to leverage these cybersecurity centers for their established enhanced coordination procedures, above-steady-state capacity, and/or operational or support personnel.

National Cybersecurity and Communications Integration Center (NCCIC)

As an operational element of the Department of Homeland Security, the NCCIC is the primary platform to coordinate the Federal Government's asset response to cyber incidents. The NCCIC is authorized under Section 3 of the National Cybersecurity Protection Act of 2014.

National Cyber Investigative Joint Task Force (NCIJTF)

The NCIJTF is a multi-agency center hosted by the Federal Bureau of Investigation and is the primary platform to coordinate the Federal Government's threat response. The NCIJTF is chartered under paragraph 31 of National Security Presidential Directive-54/Homeland Security Presidential Directive-23.

Cyber Threat Intelligence Integration Center (CTIIC)

Operated by the Office of the Director of National Intelligence, the CTIIC is the primary platform for intelligence integration, analysis, and supporting activities for the Federal Government. CTIIC also provides integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests.

U.S. Cyber Command (USCYBERCOM) Joint Operations Center (JOC)

The USCYBERCOM JOC directs the U.S. military's cyberspace operations and defense of the Department of Defense Information Network (DoDIN). USCYBERCOM manages both the threat and asset responses for the DoDIN during incidents affecting the DoDIN and receives support from the other centers, as needed.

National Security Agency Cybersecurity Threat Operations Center (NCTOC)

The National Security Agency Cybersecurity Threat Operations Center (NCTOC) is the 24/7/365 NSA element that characterizes and assesses foreign cybersecurity threats. The NCTOC informs partners of current and potential malicious cyber activity through its analysis of foreign intelligence, with a focus on adversary computer network attacks, capabilities, and exploitations. Upon request, the NCTOC also provides technical assistance to U.S. Government departments and agencies.

Department of Defense Cyber Crime Center (DC3)

DC3 supports the law enforcement, counterintelligence, information assurance, network defense, and critical infrastructure protection communities through digital forensics, focused threat analysis, and training. DC3 provides analytical and technical capabilities to federal agency mission partners conducting national cyber incident response.

⁴¹ See page 30 for description.

Intelligence Community – Security Coordination Center (IC-SCC)

The IC-SCC mission is to monitor and oversee the integrated defense of the IC Information Environment in conjunction with IC mission partners and in accordance with the authority and direction of the Office of the Director of National Intelligence Chief Information Officer. The IC - Incident Response Center roles and responsibilities were assumed upon the IC SCC's founding in 2014.

Annex F: Core Capabilities and Critical Tasks

Each core capability identified in the National Cyber Incident Response Plan (NCIRP) has critical tasks that facilitate capability execution. These critical tasks are tasks that are essential to achieving the desired outcome of the capability. Critical tasks inform mission objectives, which allow planners to identify resourcing and sourcing requirements prior to an incident. The chart below describes each core capability and identifies critical tasks associated with each capability.

Core Capabilities and Critical Tasks
<p>1. <u>Access Control and Identity Verification</u></p> <p>Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems. Also referred to as Authentication and Authorization.</p>
<p>Critical Tasks:</p> <ul style="list-style-type: none"> • Verify identity to authorize, grant, or deny access to cyber assets, networks, applications, and systems that could be exploited to do harm. • Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform audit activities to verify and validate security mechanisms are performing as intended. • Conduct training to ensure staff-wide adherence to access control authorizations.
<p>2. <u>Cybersecurity</u></p> <p>Description: Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as computer network defense, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts.</p>
<p>Critical Tasks:</p> <ul style="list-style-type: none"> • Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited. • Secure, to the extent possible, public and private networks and critical infrastructure (e.g., communication, financial, electricity sub-sector, water, and transportation systems), based on vulnerability results from risk assessment, mitigation, and incident response capabilities. • Create resilient cyber systems that allow for the uninterrupted continuation of essential functions. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Core Capabilities and Critical Tasks

3. Forensics and Attribution

Description: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.

Critical Tasks:

- Retrieve digital media and data network security and activity logs.
- Conduct digital evidence analysis, and respecting chain of custody rules.
- Conduct physical evidence collections, analysis adhere to rules of evidence collection as necessary.
- Assess capabilities of likely threat actors(s).
- Leverage the work of incident responders and technical attribution assets to identify malicious cyber actor(s).
- Interview witnesses, potential associates, and/or perpetrators if possible.
- Apply confidence levels to attribution assignments.
- Include suitable inclusion and limitation information for sharing products in attribution elements guidance.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Perform audit activities to verify and validate security mechanisms are performed as intended.

4. Infrastructure Systems

Description: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.

Critical Tasks:

- Maintain a comprehensive understanding of the needs for the safe operation of control systems.
- Stabilize and regain control of infrastructure.
- Increase network isolation to reduce the risk of a malicious cyber activity propagating more widely across the enterprise or among interconnected entities.
- Stabilize infrastructure within those entities that may be affected by cascading effects of the cyber incident.
- Facilitate the restoration and sustainment of essential services (public and private) to maintain community functionality.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Maintain up-to-date data knowledge of applicable emerging and existing security research, development, and solutions.

Core Capabilities and Critical Tasks

5. Intelligence and Information Sharing

Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.

Critical Tasks:

- Monitor, analyze, and assess the positive and negative impacts of changes in the operating environment as it pertains to cyber vulnerabilities and threats.
- Share analysis results through participation in the routine exchange of security information—including threat assessments, alerts, threat indications and warnings, and advisories—among partners.
- Confirm intelligence and information sharing requirements for cybersecurity stakeholders.
- Develop or identify and provide access to mechanisms and procedures for confidential intelligence and information sharing between the private sector and government cybersecurity partners.⁴²
- Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include critical infrastructure participants and partners with roles in physical response efforts.
- Share actionable cyber threat information with SLTT and international governments and private sectors to promote shared situational awareness.
- Enable collaboration via online networks that are accessible to all participants.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

⁴² Information sharing must provide effective communication to individuals with access and functional needs, including people with limited English proficiency and people with disabilities, including people who are deaf or hard of hearing and people who are blind or have low vision. Effective communication with individuals with access and functional needs includes use of appropriate auxiliary aids and services, such as sign language and other interpreters, captioning of audio and video materials, user-accessible Web sites, communication in various languages, and use of culturally diverse media outlets.

Core Capabilities and Critical Tasks

6. Interdiction and Disruption

Description: Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity.

Critical Tasks:

- Deter malicious cyber activity within the United States, its territories, and abroad.
- Interdict persons associated with a potential cyber threat or act.
- Deploy assets to interdict, deter, or disrupt cyber threats from reaching potential target(s).
- Leverage law enforcement and intelligence assets to identify, track, investigate, and disrupt malicious actors threatening the security of the Nation's public and private information systems.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

7. Logistics and Supply Chain Management

Description: Facilitate and assist with delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.

Critical Tasks:

- Identify and catalog resources needed for response, prior to mobilization.
- Mobilize and deliver governmental, nongovernmental, and private sector resources to stabilize the incident and integrate response and recovery efforts, to include moving and delivering resources and services to meet the needs of those impacted by a cyber incident.
- Facilitate and assist delivery of critical infrastructure components to rapid response and restoration of cyber systems.
- Enhance public and private resource and services support for impacted critical infrastructure entities.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Apply supply chain assurance principles and knowledge within all critical tasks identified above.

Core Capabilities and Critical Tasks

8. Operational Communications

Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.

Critical Tasks:

- Ensure the capacity to communicate with both the cyber incident response community and the affected entity.
- Establish interoperable and redundant voice, data, and broader communications pathways between SLTT, particularly state fusion centers, federal, and private sector cyber incident responders.
- Facilitate establishment of quickly formed ad hoc voice and data networks on a local and regional basis so critical infrastructure entities can coordinate activities even if Internet services fail.
- Coordinate with any UCG (or entity) established to manage physical (or non-cyber) effects of an incident. Ensure availability of appropriate secure distributed and scalable incident response communication capabilities including out-of-band communications mechanisms where traditional communications and/or systems are compromised. Adhere to appropriate mechanisms for safeguarding sensitive and classified information private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information.
- Protect individual privacy, civil rights, and civil liberties.
- Cyber threat information also is conducted through automated indicator sharing using established formats such as Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information (STIX/TAXII).⁴³
- Perform red team activities to verify and validate that forensics and attribution capabilities are performing as intended and have adequate visibility.

9. Operational Coordination

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities.

Critical Tasks:

- Mobilize all critical resources and establish coordination structures as needed throughout the duration of an incident.
- Define and communicate clear roles and responsibilities relative to courses of action.
- Prioritize and synchronize actions to ensure unity of effort.
- Ensure clear lines and modes of communication between entities, both horizontally and vertically.
- Ensure appropriate private sector participation in operational coordination throughout the cyber incident response cycle consistent with the NIPP.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Perform table-top activities to verify and validate effective and appropriate coordination between stakeholders.

⁴³ <https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity>

Core Capabilities and Critical Tasks

10. Planning

Description: Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

Critical Tasks:

- Initiate a flexible planning process that builds on existing plans as part of the National Planning System.⁴⁴
- Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities.
- Establish partnerships that coordinate information sharing between partners to restore critical infrastructure within single and across multiple jurisdictions and sectors.
- Inform risk management response priorities with critical infrastructure interdependency analysis.
- Identify and prioritize critical infrastructure and determine risk management priorities.
- Conduct cyber vulnerability assessments, perform vulnerability and consequence analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private and nonprofit sectors and local, regional/metropolitan, state, tribal, territorial, insular area, and federal organizations and agencies.
- Develop operational, business/service impact analysis, incident action, and incident support plans at the federal level and in the states and territories that adequately identify critical objectives based on the planning requirements; provide a complete and integrated picture of the escalation and de-escalation sequence and scope of the tasks to achieve the objectives; and are implementable within the time frame contemplated in the plan using available resources.
- Formalize partnerships such as memorandums of understanding or pre-negotiated contracts with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner.
- Formalize partnerships between communities and disciplines responsible for cybersecurity and for physical systems dependent on cybersecurity. Formalize relationships such as memorandums of understanding or pre-negotiated contracts between information communications technology and information system vendors and their customers for ongoing product cyber security, business planning, and transition to response and recovery when necessary.
- Formalize partnerships with government and private sector entities for data and threat intelligence sharing, prior to, during, and after an incident.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

⁴⁴ The National Planning System provides a unified approach and common terminology to support the implementation of the [National Preparedness System](#) through plans that support an “all threats and hazards” approach to preparedness. These plans—whether strategic, operational, or tactical—enable the whole community to build, sustain, and deliver the core capabilities identified in the [National Preparedness Goal](#).

Core Capabilities and Critical Tasks

11. Public Information and Warning

Description: Deliver coordinated, prompt, reliable, and actionable information to the whole community and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.

Critical Tasks:

- Establish accessible mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, faith-based organizations, nongovernmental organizations, and the public.
- Share actionable information and provide situational awareness with the public, private, and nonprofit sectors, and among all levels of government.
- Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System, public media, and social media sites.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect applicable information sharing and privacy protections, including Traffic Light Protocol.
- Assure availability of redundant options to achieve critical public information, threat indication, and warning outcomes.

12. Screening, Search, and Detection

Description: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.

Critical Tasks:

- Locate persons and networks associated with cyber threats.
- Develop relationships and further engage with critical infrastructure participants (private industry and SLTT partners).
- Conduct physical and electronic searches as authorized by law
- Collect and analyze information provided.
- Detect and analyze malicious cyber activity and support mitigation activities.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Core Capabilities and Critical Tasks

13. Situational Assessment

Description: Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.

Critical Tasks:

- Coordinate the production and dissemination of modeling and effects analysis to inform immediate cyber incident response actions.
- Maintain standard reporting templates, information management systems, essential elements of information, and critical information requirements.
- Develop a common operational picture for relevant incident information shared by more than one organization.
- Coordinate the structured collection and intake of information from multiple sources for inclusion into the assessment processes.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

14. Threats and Hazards Identification

Description: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of an entity.

Critical Tasks:

- Identify data requirements across stakeholders.
- Develop and/or gather required data in a timely and efficient manner to accurately identify cyber threats.
- Ensure that the right people receive the right data at the right time.
- Translate data into meaningful and actionable information through appropriate analysis and collection tools to aid in preparing the public.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Discover, evaluate and resolve gaps in policy, facilitate or enable technologies, partnerships, and procedures which are barriers to effective threat, vulnerability, and hazard identification for the sectors.

Annex G: Developing an Internal Cyber Incident Response Plan

This Annex describes processes that may be used for cyber incident response planning. The first subsection describes the national operational planning process. The second subsection outlines a planning process that individual entities may take.

National Operational Planning

An operational plan is a continuous, evolving instrument of anticipated actions that maximizes opportunities and guides response operations. Operational plans are “living documents,” subject to revision as incidents evolve and new information becomes available. Operational plans seek to:

- Improve coordination, collaboration, and communication to identify and prioritize plans of actions and steps at various thresholds of escalation surrounding a cyber incident;
- Improve the ability to gather, analyze, and de-conflict multiple sources of information to produce timely and actionable situational awareness;
- Issue alerts and warnings across a broad range of stakeholders to raise awareness and initiate incident response activities, consequence management, and business continuity plans;
- Reduce redundancy and duplication that could adversely impact effective coordination by articulating and affirming various roles and responsibilities;
- Enhance predictability and sustainability to improve collaboration necessary to manage consequences and assess and mitigate impact; and
- Include flexibility and agility to adapt to emerging events and activities.

Operational planning is conducted across the broader community and is an inherent responsibility of every level of government and the private sector. Operational plans should be routinely exercised to ensure identify gaps and establish continuous improvement plans to improve preparedness and effectiveness of the information sharing process surrounding a cyber incident.

This NCIRP is not an operational plan for responding to cyber incidents. However, it should serve as the primary strategic approach for stakeholders to utilize when developing agency- and organization-specific operational plans. This common doctrine will foster unity of effort for emergency operations planning and it will help those affected by cyber incidents to understand how federal departments, agencies, and other national-level broader community partners provide resources to support the SLTT communities and private sector response operations.

Response Operational Planning

Both the Comprehensive Preparedness Guide (CPG) 101⁴⁵ and the Response Federal Interagency Operational Plan (FIOP)⁴⁶ are foundational documents that agencies and organizations can leverage and tailor to cyber incidents to develop their own operational response plans.

⁴⁵ CPG 101, Developing and Maintain Emergency Operations Plans, Version 2. November 2010. <https://www.fema.gov/media-library/assets/documents/25975>

⁴⁶ Response Federal Interagency Operational Plan, Second Edition. August 2016. https://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf

The CPG 101 provides information on various types of plans and guidance on the fundamentals of planning. Federal plans for incidents are developed using a six-step process, in alignment with the steps described in CPG 101:

- Form a collaborative planning team
- Understand the situation
- Determine the goals and objectives
- Develop the plan
- Prepare, review, and approve the plan
- Implement and maintain the plan.

The Response FIOP outlines how the Federal Government delivers the response core capabilities. The Response FIOP provides information regarding roles and responsibilities, identifies the critical tasks an entity takes in executing core capabilities, and identifies resourcing and sourcing requirements. It addresses interdependencies and integration with the other mission areas throughout the plan's concept of operations. It also describes the management of concurrent actions and coordination points with the areas of prevention, protection, mitigation, and recovery. It does not contain detailed descriptions of specific department or agency functions, as such information is located in department- or agency-level operational plans.

The NRF and NIMS guide the Response FIOP. The NRF is based on the concept of tiered response, with an understanding that most incidents start at the local and tribal level, and as needs exceed resources and capabilities, additional SLTT and federal assets are applied. The Response FIOP, therefore, aligns with other SLTT, insular area, and federal plans to ensure that all response partners share a common operational focus. Similarly, integration occurs at the federal level among the departments, agencies, and nongovernmental partners that compose the respective mission area through the frameworks, FIOPs, and departmental and agency operations plans.

Application

While the NRF does not direct the actions of other response elements, the guidance contained in the NRF and the Response FIOP informs SLTT and insular area governments, as well as nongovernment organizations and the private sector, regarding how the Federal Government responds to incidents. These partners can use this information to inform their planning and ensure that assumptions regarding federal assistance and response, and the manner in which federal support will be provided, are accurate.

Developing an Internal Cyber Incident Response Plan

Public and private sector entities should consider creating an entity-specific operational cyber incident response plan to further organize and coordinate their efforts in response to cyber incidents. Each organization should consider a plan that meets its unique requirements and relates to the organization's mission, size, structure, and functions.

The National Institute of Standards and Technology Special Publication 800-61 (revision 2)⁴⁷ outlines several elements to consider when developing a cyber incident response plan. Each plan should be tailored and prioritized to meet the needs of the organization and adhere to current information sharing and reporting requirements, guidelines, and procedures, where they exist. As

⁴⁷ NIST SP 800-61 Revision 2, Computer Incident Handling Guide. August 2012.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

appropriate, public and private sector entities are encouraged to collaborate in the development of cyber incident response plans to promote shared situational awareness, information sharing, and acknowledge sector, technical, and geographical interdependences.

The elements below serve as a starting point of important criteria to build upon for creating a cyber incident response plan:

- Mission
- Strategies and goals
- Organizational approach to incident response
- Risk assessments
- Cyber Incident Scoring System/Criteria⁴⁸
- Incident reporting and handling requirements
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization
- Communications with outside parties, such as:
 - Customers, constituents, and media
 - Software and support vendors
 - Law enforcement agencies
 - Incident responders
 - Internet service providers
 - Critical infrastructure sector partners
- Roles and responsibilities (preparation, response, recovery)
 - State Fusion Center
 - Emergency Operations Center
 - Local, regional, state, tribal, and territorial government
 - Private sector
 - Private citizens
- A training and exercise plan for coordinating resources with the community
- Plan maintenance schedule/process.

⁴⁸ The NCCIC Cyber Incident Scoring System could be used as a basis for an organizations operations center to assist in the internal elevation of a particular incident. <https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System>.

Annex H: Core Capability/NIST Cybersecurity Framework/PPD-41 Crosswalk

The NCIRP Crosswalk describes the relationship between the NIST Cybersecurity Framework and PPD-41. By walking through the table below, each core capability is cross-referenced to ensure continuity and connection between the three documents. This table should be leveraged as a starting point that may assist in the NCIRP’s response activities under each core capability, understanding the NIST’s functions and categories, and the PPD’s respective Lines of Effort.

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
Access Control and Identity Verification	Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.		Access Control Protective Technology				Asset Response
Cybersecurity	Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation.	Asset Management Business Environment Risk Assessment Risk Management Strategy	Access Control Data Security Information Protection Processes and Procedures Protective Technology	Anomalies and Events Security Continuous Monitoring Detection Processes	Communications Response Planning Analysis Mitigation	Communications Improvements Recovery Planning	Asset Response
Forensics and Attribution	Forensic investigations and efforts to provide attribution for an incident are complimentary functions that often occur in parallel during a significant cyber incident.				Analysis		Threat Response Asset Response Intelligence Support

National Cyber Incident Response Plan

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
Infrastructure Systems	Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.	Asset Management Business Environment Risk Assessment	Access Control Data Security Information Protection Processes and Procedures Protective Technology	Anomalies and Events Security Continuous Monitoring Detection Processes		Communications Improvements Recovery Planning	Asset Response
Intelligence and Information Sharing	Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.	Asset Management Business Environment	Awareness & Training Data Security	Security Continuous Monitoring Detection Processes	Communications Analysis Mitigation Improvements	Communications	Threat Response Asset Response Intelligence Support
Interdiction and Disruption	Delay, divert, intercept, halt, apprehend, or secure threats						Threat Response

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
	related to malicious cyber activity.						
Logistics and Supply Chain Management	Facilitate and assist with delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.	Business Environment					Asset Response
Operational Communications	Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between entities affected by the malicious cyber activity and all responders.	Asset Management		Communications	Communications		Threat Response Asset Response Intelligence Support
Operational Coordination	Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports execution of core capabilities.	Governance Risk Assessment Risk Management	Anomalies and Events				Threat Response Asset Response Intelligence Support
Planning	Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic,				Response Planning	Recovery Planning Improvements	Threat Response Asset Response

National Cyber Incident Response Plan

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
	operational, and/or tactical-level approaches to meet defined objectives.						Intelligence Support
Public Information and Warning	Deliver coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.				Communications	Communications	Threat Response Asset Response Intelligence Support
Screening, Search and Detection	Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures.			Anomalies and Events Security Continuous Monitoring Detection Processes			Threat Response Asset Response Intelligence Support
Situational Assessment	Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response. In the context of a cyber	Business Environment Communications Awareness and Training		Detection Processes	Communications	Communications	Threat Response Asset Response Intelligence Support

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
	incident, this capability focuses on rapidly processing and communicating large quantities of information from across the whole community from the field-level to the national-level to provide all decision makers with the most current and accurate information possible.						
Threats and Hazards Identification	Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of an entity.			Anomalies and Events Security Continuous Monitoring Detection Processes			Threat Response

Annex I: Additional Resources

The following resources can be leveraged by both the private and public sector. Entities can use this list as a starting point for understanding cyber incident response, vulnerability updates, data breach information, risk management, and organizations that serve as a points of contacts for the public and private sector. This non exhaustive alphabetical list provides a wide range of information that can also be leveraged beyond the scope of this document.

- Center for Internet Security: www.cisecurity.org
- CIS Critical Controls: <https://www.cisecurity.org/critical-controls.cfm>
- Cyber Incident Severity Schema: <https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf>
- DHS Critical Infrastructure Cyber Community Voluntary Program: <https://www.us-cert.gov/ccubedvp>
- Government Coordinating Councils: <https://www.dhs.gov/gcc>
- Information Sharing and Analysis Organizations: <https://www.isao.org/>
- Infragard: www.infragard.org
- Industrial Control System Security Computer Emergency Response Team: <https://ics-cert.us-cert.gov>
- Malware Investigator: <https://www.malwareinvestigator.gov/>
- MITRE Common Vulnerabilities and Exposures: <https://cve.mitre.org/>
- Multi-State Information Sharing and Analysis Center: <https://msisac.cisecurity.org/>
- National Council of Information Sharing and Analysis Centers: <http://www.nationalisacs.org/>
- National Incident Management System: <https://www.fema.gov/national-incident-management-system>
- National Vulnerability Database: www.nvd.nist.gov
- NIST Framework for Improving Critical Infrastructure Cybersecurity: <https://www.nist.gov/cyberframework>
- NIST National Checklist Program Repository: <https://web.nvd.nist.gov/view/ncp/repository>
- NIST SP 800-61:: Revision 2: Computer Incident Handling Guide: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- NIST SP 800-37: Guide to Applying the Risk Management Framework to Federal Information Systems: <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
- NVD Common Vulnerability Scoring System: <https://nvd.nist.gov/cvss.cfm> Sector Coordinating Councils: <https://www.dhs.gov/scc>
- US-CERT Website: www.us-cert.gov

Annex J: Acronym List

CRG	Cyber Response Group
CTIIC	(Office of the Director of National Intelligence) Cyber Threat Intelligence Integration Center
DC3	Department of Defense Cyber Crime Center
DHS	Department of Homeland Security
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DoDIN	Department of Defense Information Network
DOJ	Department of Justice
DOS	Department of State
ESF	Emergency Support Functions
FBI	(Department of Justice) Federal Bureau of Investigations
FEMA	(Department of Homeland Security) Federal Emergency Management Agency
GCC	Government Coordinating Council
HSI	(Department of Homeland Security) Homeland Security Investigations
IC	Intelligence Community
IC3	Internet Crime Complaint Center
IC-SCC	Intelligence Community Security Coordination Center
ICE	(Department of Homeland Security) Immigrations and Customs Enforcement
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organization
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
JOC	Joint Operations Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCIRP	National Cyber Incident Response Plan
NCCIC	(Department of Homeland Security) National Cybersecurity and Communications Integration Center
NCIJTF	(Federal Bureau of Investigations) National Cyber Investigative Joint Task Force
NCPA	National Cybersecurity Protection Act
NCTOC	National Security Agency Cybersecurity Threat Operations Center
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology

NIPP	National Infrastructure Protection Plan
NRF	National Response Framework
ODNI	Office of the Director of National Intelligence
PII	Personally Identifiable Information
PPD	Presidential Policy Directive
SCC	Sector Coordinating Council
SLTT	State, Local, Tribal, and Territorial
SLTT GCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	Sector Specific Agency
UCG	Unified Coordination Group
US-CERT	United States – Computer Emergency Readiness Team
USCYBERCOM	(Department of Defense) United States Cyber Command



Homeland Security

THE HOMELAND SECURITY *NEWS BRIEFING*

PREPARED FOR THE DEPARTMENT OF HOMELAND SECURITY BY BULLETIN INTELLIGENCE WWW.BULLETININTELLIGENCE.COM/DHS

TO: THE SECRETARY AND SENIOR STAFF
DATE: THURSDAY, JANUARY 19, 2017 5:00 AM EST

TODAY'S EDITION

Leading DHS News

Security Officials Making Final Preparations For Inauguration.....	4
Court Orders Four DHS Officials To Preserve Private-Account Emails.....	4
Senate Democrats Say Gen. Kelly May Be Confirmed Friday.....	4

Immigration and Customs Enforcement

Hunter Proposes Bill To Deprive "Sanctuary" Colleges Of Federal Funds.....	5
New York AG To Offer Guidance For "Sanctuary" Cities.....	5
Massachusetts Sheriffs Sign 287(g) Agreements.....	5
Opinion: Supreme Court Cases May Affect Trump's Ability To Engage In Mass Deportations.....	5

Customs and Border Protection

Border Patrol Arrests Over 1,000 People In Operation Targeting Human Smuggling Since October.....	5
CAIR Files Complaints With CBP, DHS, DOJ Over Interrogation Questions.....	6
Continuing Coverage: Two Arizona Teens Charges With Firing At Border Patrol Vehicle.....	6
Continuing Coverage: Border Patrol Agent's Murder Trial Begins.....	6
LATimes: Texas Should Not Be Reimbursed By US For Patrolling Border.....	6

Transportation Security Administration

Administrator Neffenger Reviews Tenure.....	6
Continuing Coverage: Actor Judge Reinhold Pleads No Contest To Airport Disorderly Conduct.....	6

Federal Emergency Management Agency

\$4.5 Million FEMA Grant To Be Used For Hurricane Matthew Recovery Process In North Carolina.....	6
Heavy Rainfall Triggers Flash Flooding In Houston.....	7
Former Agency Official Urges Next Administrator To Eliminate FEMA Corps Program.....	7

US Citizenship and Immigration Services

Obama Says He Would Speak Out On "Round Up" Of Dreamers Under Trump.....	7
Mayors Group Calls For Immigration Reform, Protection For Dreamers.....	8
Afghan Translators Visa Program Backlog Leaves Many In Fear For Their Lives.....	8

Immigration

Feds Answer Questions Regarding Policy Change On Cuban Migrants.....	8
Haley "Repudiates" Muslim Registry Idea Under Trump.....	8
Fed Dallas President Kaplan Says Immigration Makes US Stronger.....	8
PRI: More Mexicans Leaving US For Mexico.....	9

US Coast Guard

Coast Guardsman Attending Training Course Dies.....	9
Coast Guard To Install Additional Radio Activation Switches At Maine Lighthouses.....	9

Secret Service

DisruptJ20 Protest Group Vows To Disrupt Inauguration Events.....	9
---	---

Man Appears To Have Set Himself On Fire Outside Trump Hotel In DC.	9
Florida Man Charged With Threatening To Kill Trump.	9
Continuing Coverage: Secret Service Settles Discrimination Case.	10
Pence Motorcade Injures DC Police Officer.....	10

National Protection and Programs

Protective Security Service Officer Accidentally Shoots Self In Leg.	10
Minnesota Lawmakers To Consider Real ID Compliance Legislation.	10
South Carolina Visitors To Fort Bragg May Use Licenses Until June.	10
Stop The Bleed Program Introduced In Des Moines.	10

Terrorism Investigations

Justices Appear To Favor Bush Administration Officials In 9/11 Detainee Case.	10
FBI Probing Second Wave Of Bomb Threats To Jewish Community Centers.	11
Pence: Americans’ Safety, Security Is Trump’s Top Priority.	11
Trump Expected To Seek Reform Of Intelligence Community.....	12
In Mali, Truck Bomb Kills 60, Injures More Than 100 At Army Base.....	12
Guantanamo Bay Detention Center Remains Open As Obama Exits Stage.....	12
Widow Of Orlando Nightclub Gunman Pleads Not Guilty.....	12
Suspect Arrested For Allegedly Communicating Fake Bomb Threat To Flight Crew.	12
Algerian Gitmo Detainee’s Transfer Appeal Denied.	12
Judge Rules DOD Must Release Abu Ghraib Photos.	13

Cyber News

DHS Releases Updated National Cyber Incident Response Plan.	13
Senate Armed Services Committee Creates Cybersecurity Standing Subcommittee.....	13
State Officials Felt “Blindsided” By Decision To Designate Elections Systems As Critical Infrastructure.	13
Chaffetz Requests Information On “Unauthorized Scans” Of Georgia Secretary Of State Firewall.....	13
Cyber Expert Highlights Animal-Caused Outages To Bring Perspective To Cyber Debate.	13
GCHQ Establishes Cyber Contest For Teenage Girls.....	13
White House Cybersecurity Coordinator Defends Obama’s Cyber Legacy.....	14
Researchers Develop Protocol To Update Automobile Software To Reduce Hacking Vulnerability.	14
Sheth: Government Procurement, Budget Woes Lead To Insufficient Cybersecurity.	14
Participants In Florida Cyber Contest Represent Eight-Fold Boost In Participation History.....	14
Cyberweapons Deal Between Company, Mauritanian Government Devolves Into “International Incident.”	14
Ukrainian Utility: December Power Outage In Kiev Caused By Cyberattack.....	15
Gallagher: Trump Favors “Aggressive” Cyber Posture, But Cyber Policies Unclear.	15
Poroshenko Calls For Global Response To Russian Hacking.	15

National Security News

JCS Chairman Says Options In Fight Against ISIL Are Ready For New Administration.	15
US Says Coalition Has Enough Local Arab Fighters To Move On Raqqa.....	15
Russia Announces Joint Airstrikes With Turkey On ISIL Positions Around Al-Bab.	15
Iraq Announces It Has Control Of Eastern Half Of Mosul.....	15
WPost Analysis: Trump Faces Decisions About US Role In Afghanistan.....	16
Chinese President Continues Theme Of Global Cooperation At UN.	16
Obama Warns Moving US Embassy To Jerusalem Could Be “Explosive.”	16
Power: UN Needs To “Push” Iran On Arms Embargo.	17
Biden, Stoltenberg Push Back Against Trump’s Claim NATO Is “Obsolete.”	17
Sources: FBI, Other Agencies Investigating Possible Kremlin Aid To Trump.....	17
Pence Downplays Concerns Over Trump Team’s Foreign Policy Preparedness.	18
Russia Extends Snowden’s Asylum.....	18
Pence Says Assange Will Be Held Accountable If Extradited To US.	18
European Leaders Seek To Meet With Trump Before Putin.	19
Jammeh Faces Midnight Deadline To Step Down.....	19
South Korean Court Rejects Arrest Of Samsung Heir In Corruption Case.	19
Rights Groups Ask China To Free Tibetan Advocate.....	19

Pakistani Jailed Doctor Thought To Have Helped CIA With Bin Laden Won't Be Freed..... 19

National News

Media Analyses: Obama Sends Message To Trump During Final Press Conference..... 19
Trump To Deliver "Very Personal" Inauguration Address..... 21
Mattis Easily Clears Armed Services Committee..... 22
Trump Says His Healthcare Plan Will Be Less Expensive Than ACA..... 22
Pence: ACA Replacement Plan "Coming Together."..... 22
Alexander Says ACA Repeal Should Not Happen Until Replacement Is Ready..... 23
Cuomo Says ACA Repeal Could Hurt New Yorkers..... 23
NIH Director's Response To Fungus In Medicine Vials Comes Under Criticism..... 23
Senators Criticize DEA's Enforcement Efforts Against Opioid Distributors..... 23
Donors Announce \$500 Million For Organization To Combat Epidemics..... 23
Ryan, Bannon Collaborating On Tax Reform Plan..... 23
Haley Expresses Differences With Trump During Confirmation Hearing..... 24
Ross: Renegotiating NAFTA Will Be Trump Administration's First Trade Priority..... 24
Price Vows To Protect Access To Health Coverage, Denies Investment Wrongdoing..... 24
Mulvaney Failed To Pay Employment Taxes For Household Worker..... 25
Media Analyses: Pruitt Takes Aggressive Stance During Confirmation Hearing..... 25
NYTimes Analysis: Perry "Initially Misunderstood" Role Of Energy Secretary..... 26
Media Analyses: DeVos Faced "Bumpy" Hearing, Appeared Unprepared..... 26
McCain Says He Remains "Very Concerned" About Tillerson..... 26
Former OneWest Mortgage Customers Come To Capitol Hill To Criticize Mnuchin..... 26
Trump To Nominate Perdue For USDA..... 27
Army Secretary Nominee Was Accused Of Punching Concessions Worker Last Summer..... 27
Commodity Futures Trading Commission Enforcement Chief Stepping Down..... 27
Trump Has Not Selected Official White House Photographer..... 27
Christie Says He Turned Down Several Posts Because Of Wife's Objections..... 27
Ways And Means Chairman Defends "Border-Adjustable Tax Provision."..... 27
USA Today Analysis: Recent Job Announcements Partly Effort To Gain Favor With Trump..... 27
Chicago Police Officer Charged With First-Degree Murder In Off-Duty Shooting..... 28
Obama Administration Races To Finish Corporate Probes..... 28
Labor Department Sues Oracle, Claiming It Pays White Men More Than Others..... 28
JPMorgan Chase Settles Investigation Over Discriminatory Lending..... 28
CFPB Lawsuit Says Navient Cheated Borrowers..... 28
ED Drops "Supplement Not Supplant" Rule Under "Every Student Succeeds" Act..... 28
Media Analyses Ponder Obama's Legacy..... 28
Obamas To Vacation In Palm Spring Following Trump's Inauguration..... 29
Trump Insiders Expect "Wild First Week," "Shock And Awe Strategy" With Executive Actions..... 29
Bush 41, Wife Hospitalized In Texas..... 29
Trump A Target At DNC Candidates Forum..... 29
Quinnipiac Poll: Clinton Would Beat De Blasio In NYC Mayoral Race..... 30
NASA, NOAA Say 2016 Was Hottest Year On Record..... 30
Group Plans \$10 Million Campaign On Behalf Of Trump's Supreme Court Nominee..... 30
Pence Likens Trump To Reagan..... 30
Pence Praises Obama Administration's Handling Of Transition..... 31
Trump Delivers "Free Flowing" Speech At Dinner Honoring Pence..... 31
Trump Won't Move White House Press Briefing Room, But Will Choose Who Gets In..... 31
Yellen: Fed Will Not Be Deterred By "Short-Term Political Pressures."..... 31
Experts Say Trump's Plan For Business Assets Leaves Unanswered Questions..... 32
Trump Pays \$25 Million To Settle Trump University Suit..... 32
65 House Democrats Say They'll Boycott Trump's Inauguration..... 32
Ahead Of Women's March On Washington, A "Bitter Rift" Over Abortion..... 33
Trump Calls Mar-A-Lago His "Winter White House."..... 33
Cuomo Tells Trump New York Would Suffer From Cuts In Federal Aid..... 33

Politico Analysis: Big City Mayors Attack Trump In Hopes Of Boosting Their Profiles.....	33
After Murder Of DNC Aide Rich, Conspiracy Theories Ran Amok.....	33
Research Casts Doubt On Influence Of Fake News On Election Result.....	34
Congressional Republicans Plan Measures To Reverse Some Local DC Policies.....	34
High Court Appears Skeptical Of Law Banning Offensive Trademarks.....	34
Failed Supreme Court Nominee Garland Returns To Federal Bench.....	34
Missouri, New Hampshire Taking Up “Right-To-Work” Bills.....	34

The Big Picture

Headlines From Today’s Front Pages.....	34
---	----

Washington's Schedule

Today’s Events In Washington.....	35
-----------------------------------	----

Last Laughs

Late Night Political Humor.....	37
---------------------------------	----

LEADING DHS NEWS

Security Officials Making Final Preparations For Inauguration.

The [New York Times](#) (1/18, Fandos, Subscription Publication, 13.9M) reports, “Law enforcement officials are in the final stages of sealing off a heavily fortified security zone encompassing the Capitol and the historic National Mall here as they prepare for” President-elect Trump’s “inauguration on Friday and the substantial protests it is expected to attract.” Along with “the usual range of threats, officials” are getting ready “for what they say could be large-scale protests aimed at disrupting the” inauguration and expressing dissatisfaction with “Trump’s presidency at the moment the world is watching his ascension to office.” The threats “are making this week’s festivities the most difficult security challenge since the inauguration of President Obama in 2009.” The Times quotes Secretary Johnson from a briefing last week where he said, “We’ve got to be vigilant, we’ve got to plan, we’ve got to prepare.” Johnson “said inaugural planners have been particularly attentive to the threats of self-radicalized, so-called lone wolf terrorists this time, given the evolution of the global terrorism threat in the last four years.” The Times adds that the security forces will include “10,000 representatives from the Department of Homeland Security, including the United States Coast Guard, Secret Service and Transportation Security Administration.”

[U.S. News & World Report](#) (1/18, Cakir, 1.02M) reports security at the inauguration will be “more intense this year as officials prepare to protect the new president and an anticipated crowd of 800,000 to 900,000 from new threats: weaponized drones, thousands of protesters, terrorists, trucks plowing through crowds and cyberattacks.” The security effort “will be headquartered at the Multi Agency Communication Center in northern Virginia, where dozens of experts from local and federal agencies will monitor the events.” Security

forces are also preparing to “handle the high number of protesters expected,” which could be as high as “10 times the average at past inaugurations, officials said.” Secretary Johnson is quoted as saying, “As long as they are nonviolent, [protesters] will be allowed to exercise their First Amendment rights.”

Court Orders Four DHS Officials To Preserve Private-Account Emails.

[Politico](#) (1/18, Gerstein, 2.46M) reports, in its “Under The Radar” blog, US District Court Judge Randolph Moss ordered “four current or former top officials at the Department of Homeland Security, including Secretary Jeh Johnson, to preserve emails in their private accounts that may be responsive to a Freedom of Information Act lawsuit.” The officials also include former Deputy Secretary Alejandro Mayorkas, former Chief of Staff Christian Marrone, and former General Counsel Stevan Bunnel. Moss “issued the order Wednesday morning...telling them to copy relevant messages to thumb drives.” The Judge “said the Justice Department indicated that all four men agreed to preserve any responsive messages that might be in their private accounts, but he still granted the preservation order sought by the conservative group Judicial Watch, which said it feared the government might lose easy access to the records as Obama appointees ship out.” Moss is quoted as saying the “Court has no reason to doubt that the four individuals have agreed to comply fully with their obligations to preserve any potentially responsive emails and that they have every intention of doing so.” He added that the order was issued “out of the abundance of caution.”

Senate Democrats Say Gen. Kelly May Be Confirmed Friday.

[Bloomberg Politics](#) (1/18, Dennis, 201K) reports that Senate Democrats say four Cabinet nominees – Transportation Secretary-designate Elaine Chao, DHS Secretary-designate John Kelly, Defense Secretary-

designate James Mattis, and CIA Director-designate Mike Pompeo – could be confirmed on Inauguration Day Friday.

IMMIGRATION AND CUSTOMS ENFORCEMENT

Hunter Proposes Bill To Deprive “Sanctuary” Colleges Of Federal Funds. The [Washington Times](#) (1/18, Dinan, 272K) reports in response to “dozens” of colleges and universities declaring themselves unwilling to cooperate with federal immigration authorities, Rep. Duncan Hunter (R-CA) has introduced a bill to threaten federal funds to such schools. The bill would require the Department of Homeland Security to send a list of such schools to the Department of Education which would “cancel federal payments for student loans and financial aid.” The University of California may be “the biggest target” since University President Janet Napolitano in November “ordered schools and their police departments not to undertake any efforts to enforce federal immigration laws.”

Bowling Green President Refuses Sanctuary Designation. The [AP](#) (1/19) reports Bowling Green State University President Mary Ellen Mazey said that she will not designate the college as a “sanctuary campus.” Mazey “announced Tuesday she wouldn’t go against federal law as the school’s faculty senate prepared to consider a resolution in support of the designation.” Mazey added that she has signaled support for the BRIDGE Act, which would provide protections for DACA recipients.

New York AG To Offer Guidance For “Sanctuary” Cities. The [New York Times](#) (1/18, Yee, Subscription Publication, 13.9M) reports New York Attorney General Eric T. Schneiderman, on Thursday, plans to announce “legal guidance to local governments detailing how they can resist cooperating with the federal immigration authorities.” The Times points out that California, Connecticut, Rhode Island, and Vermont have legislation restricting cooperation by local authorities with federal immigration authorities. Meanwhile, the Suffolk County sheriff’s has promised to cooperate with federal authorities even without judicial warrants. Schneiderman will offer advice on “situations in which Immigration and Customs Enforcement or Customs and Border Protection...ask local agencies for help.”

Trump Administration Could Cut Funding, Block Policies Of “Sanctuary Cities.” The [Washington Post](#) (1/18, 11.43M) reports cutting funding the “sanctuary cities” is just one way that President-elect Trump can get these places to “help with deportation.” Citing Center for Immigration Studies policy director Jessica Vaughan, the Post says

Trump can also “seek an injunction in federal court to block specific policies, especially in jurisdictions that ‘will not cooperate in any way with ICE.’” She also notes that Chicago, Seattle and San Francisco are the “worst offenders,” with “sanctuary policies that go beyond rejecting detainer requests.”

Massachusetts Sheriffs Sign 287(g) Agreements. The [Boston Herald](#) (1/19, 509K) reports Bristol County, Massachusetts Sheriff Thomas M. Hodgson signed a 287(g) partnership agreement yesterday with ICE assistance director of enforcement Matt Albence. The Herald says Hodgson’s “longstanding dream of being authorized by U.S. Immigration and Customs Enforcement to screen foreign-born arrestees for possible deportation will become a reality in the next four to six months.” Plymouth County, Massachusetts Sheriff Joseph McDonald Jr. also signed a 287(g) agreement. ICE “reports it has 287(g) agreements with more than 30 law enforcement agencies in 16 states.”

Opinion: Supreme Court Cases May Affect Trump’s Ability To Engage In Mass Deportations. In an op-ed for [The Atlantic](#) (1/17, Epps, 5.35M), University of Baltimore constitutional law professor Garrett Epps argues that two current Supreme Court cases, *Jennings v. Rodriguez* and *Ashcroft v. Abbasi*, may limit President-elect Trump’s efforts to “engage in mass deportations” of undocumented immigrants. The *Jennings* case “concerns whether aliens being detained pending deportation are entitled to a bail hearing and to release while their cases (or their appeals) are pending.” The *Ashcroft* case “asks whether official immunity would shelter a government policy of detaining aliens in abusive or sub-standard conditions.”

CUSTOMS AND BORDER PROTECTION

Border Patrol Arrests Over 1,000 People In Operation Targeting Human Smuggling Since October. The [San Diego Union-Tribune](#) (1/18, 496K) reports on a Border Patrol “effort to thwart human smuggling near Dulzura has led to the arrests of more than 1,000 people accusing of crossing into the U.S. illegally since mid-October, authorities said Wednesday.” Border Patrol agent and task force commander Matthew Dreyer said, “Smugglers are exploiting the most rugged terrain in the county, and we’re countering with this effort.” Task Force Otay, Dreyer said, aims to “deny smugglers this area as a place where they can profit off of human beings.”

CAIR Files Complaints With CBP, DHS, DOJ Over Interrogation Questions.

[International Business Times](#) (1/18, Kreiter, 814K) reports the Council on American-Islamic Relations on Wednesday indicated “it had filed a series of complaints with federal agencies, protesting what it described as the ‘systematic questioning’ of Muslim-Americans about their religious and political views.” The complaints were filed with CBP, DHS, and the Justice Department by chapters in Florida, California, and New York. The article highlights a number of the questions CAIR said were included in interrogations.

Continuing Coverage: Two Arizona Teens Charged With Firing At Border Patrol Vehicle.

In continuing coverage, [Fox News](#) (1/18, 11.07M) reports two teens in Arizona were charged after “allegedly shooting at a parked U.S. Border Patrol truck last month near Sierra Vista.” The Cochise County Sheriff’s Office “says they are from Hereford and face charges of endangerment and felony criminal damage.”

Continuing Coverage: Border Patrol Agent’s Murder Trial Begins.

In continuing coverage, the [Rio Grande Valley \(TX\) Morning Star](#) (1/18, 68K) reports the first day of Border Patrol Agent Joel Luna’s murder trial featured arguments “over evidence Tuesday morning before jury selection began in the afternoon.” The judge “turned down [Luna’s] bid to have potentially damaging testimony thrown out.” The defense tried to “suppress a statement [Luna] gave police after they seized a safe – later found with cocaine and cash inside – from his mother-in-law’s house.” Judge Benjamin Euresti “also gave prosecutors a green light to call as a witness a DNA analyst, despite defense objections that the state did not give them the required advance notice.” The Morning Star adds that the defense scored a “partial victory” when the “judge agreed not to allow prosecutors to refer to [co-defendant] Eduardo Luna’s immigration status.”

LATimes: Texas Should Not Be Reimbursed By US For Patrolling Border.

The [Los Angeles Times](#) (1/18, Board, 4.52M) editorializes that the state of Texas should not be reimbursed by the US for their “\$2.8-billion bill for Texas’ decision – unbidden by the federal government – to send National Guard troops and state law-enforcement personnel to protect the Mexican border.” The Times says Texas’ decision to send additional troops to the border was “little more than political posturing,” as the “program began at a time when border crossings were actually going down, but coincided with...Rick Perry’s campaigns for state governor.” The deployments “were made without prior agreement by federal officials to underwrite any of the costs, and the program exceeds state responsibility.” The Times concludes

that “Congress and the incoming Trump administration should stamp ‘return to sender’ on whatever invoice Texas may ultimately deliver to Washington.”

TRANSPORTATION SECURITY ADMINISTRATION

Administrator Neffenger Reviews Tenure.

[Politico Morning Transportation](#) (1/18, Gurciullo, 12K) reports TSA Administrator Neffenger participated in an interview with Politico’s Jen Scholtes this week and “looked back on a tenure at an agency that was outed for major failures just before he took the helm a year and a half ago.” He said it was surprising “how quickly you can really turn things around.” Neffenger added, “I think we made a lot of dramatic progress in the last 18 months...It’s a fundamentally different agency now. I’m convinced of that. It’s got ways to go. Every agency will continue to have ways to move forward. But we reconnected to the industry we serve, recognized that we’re actually part of that industry, not just something that stands in the middle. And as that industry – the airlines and the airports – have become more efficient at moving people, TSA had to be part of that.”

Continuing Coverage: Actor Judge Reinhold Pleads No Contest To Airport Disorderly Conduct.

In continuing coverage, the [Fort Worth \(TX\) Star-Telegram](#) (1/18, 463K) reports actor Judge Reinhold “has pleaded no contest to a misdemeanor disorderly conduct charge stemming from his arrest at Love Field airport last month, according to the Dallas Morning News.” Reinhold “received deferred adjudication Tuesday, meaning the charge will be dismissed if he avoids trouble in Dallas for 90 days.” He was arrested on December 8 for “causing a disturbance” with TSA agents and “refusing to comply with a security screening, police said.” He is quoted as saying, “I am sorry for being such a dumb – with the TSA, and I continue to admire and support the work of the Dallas Police Department.”

FEDERAL EMERGENCY MANAGEMENT AGENCY

\$4.5 Million FEMA Grant To Be Used For Hurricane Matthew Recovery Process In North Carolina.

The [AP](#) (1/18) reports North Carolina Gov. Roy Cooper announced on Wednesday that FEMA has awarded a \$4.5 million grant to his state’s emergency management office. According to the article, the money will be used to help displaced Hurricane Matthew survivors. The [Fayetteville \(NC\)](#)

[Observer](#) (1/18, Woolverton, 142K) reports Cooper said the grant money will help Matthew survivors navigate the sometimes “complex process to access safe housing and funds to repair damaged homes.” Cooper’s remarks are also highlighted by the [Stanly \(NC\) News Press](#) (1/18, Selvy-Mullis, 27K) and the [WXII-TV](#) Winston-Salem, NC (1/18, 69K) website. [WCTI-TV](#) Greenville, NC (1/18, 2K) also has online coverage of this story.

Heavy Rainfall Triggers Flash Flooding In Houston. [NBC Nightly News](#) (1/18, story 9, 0:20, Holt, 16.61M) reported that emergency response officials in Houston said they received dozens of water rescue calls after “powerful storms triggered widespread flash floods” in Houston on Wednesday. The [CBS Evening News](#) (1/18, story 9, 0:15, Pelley, 11.17M) reported, “Dozens were rescued from cars” after heavy rainfall turned some Houston “roads into rivers.” [ABC World News Tonight](#) (1/18, story 6, 1:05, Muir, 14.63M), which aired a similar report on flooding in Houston, also pointed out that stormy weather posed a threat to California and some other coastal states in the western US on Wednesday night.

Former Agency Official Urges Next Administrator To Eliminate FEMA Corps Program. In an op-ed for [The Hill](#) (1/18, 1.25M) “Pundits” blog, former FEMA Director of Intergovernmental Affairs Christopher E. Hagerup urges Administrator Fugate’s successor to implement several changes at the agency, including the elimination of the FEMA Corps program, in part because, as he puts it, many program “participants are less interested in emergency management careers than in avoiding college.”

US CITIZENSHIP AND IMMIGRATION SERVICES

Obama Says He Would Speak Out On “Round Up” Of Dreamers Under Trump. [Bloomberg Politics](#) (1/18, Talev, 201K) reports President Obama at his final news conference on Wednesday said “he would use his public platform as an ex-president to oppose any effort by the incoming Trump administration to ‘round up’ undocumented immigrants who arrived in the US as children.” While noting that he will largely attempt to stay out of public debate while President-elect Trump “settles onto office,” he also noted that he “would act to defend what he considers the nation’s ‘core values,’ including opposition to deporting such immigrants.”

Obama noted that Dreamers “for all practical purposes are American kids,” the [Los Angeles Times](#) (1/18, 4.52M) reports. “The notion that we would just arbitrarily or because

of politics punish those kids, when they didn’t do something themselves ... would merit my speaking out,” he said.

People Covered Under DACA May Receive “Paroled” Status From DHS. The [New York Times](#) (1/18, Robbins, Subscription Publication, 13.9M) reports that under the Deferred Action for Childhood Arrivals program, some are receiving a “PAROLED” stamp from the Department of Homeland Security on passports. Because of the stamp on a passport, holders may have a “far easier” time of adjusting their immigration status in the future. The Times reports that 22,340 of those covered by DACA have received the stamp. The Times highlights a six-day trip organized by the City University of New York to send Dreamers to Mexico, with each returning legally with a stamp in their passports, which it says they “are hoping could one day be inoculation against whatever actions Donald J. Trump takes against undocumented immigrants after his inauguration on Friday.”

Trump Promises Immigration Plan For Dreamers With “A Lot Of Heart.” [Politico](#) (1/18, Nelson, 2.46M) reports President-elect Trump in a Tuesday interview with Fox News’ Ainsley Earhardt “promised a revamped immigration plan that is both ‘very firm’ but also will ‘have a lot of heart’ for undocumented immigrants in difficult situations.” When asked about his plans and about the predicament of Dreamers who were brought to the US as children, “Trump said ‘I understand that,’ and said an immigration plan is in the works, set to be delivered ‘over the next two to three months.’”

DACA Students Express Concern Over Fate Of DACA Under Trump. [NPR](#) (1/18, 1.92M) reporter Ari Shapiro spoke with people in North Carolina and Virginia in the lead-up to President-elect Trump’s inauguration, asking what concerns they have “as the country faces dramatic changes.” Speaking with an undocumented political science student at Virginia Tech, Juan de la Rosa Diaz, the article says he worries about the fate of the DACA program under President-elect Trump and what that means for his education plans. He said, “I very much consider myself woven into the fabric of this country, because it’s taught me everything I know, it’s given me so many opportunities.”

Similarly, the [Louisville \(KY\) Courier-Journal](#) (1/18, Kenning, 328K) reports that undocumented student Jennifer Neria Escamilla, who is “now close to earning a bachelor’s degree at the University of Kentucky,” is one of thousands who are “worried the new president will sweep away protections that helped her get college scholarships, gain a work permit and ease worries about deportation.” She said, “My biggest fear is for him to take away DACA and not be able to finish my degree...I already couldn’t study abroad.” The article notes, however, “there have been some signs Trump’s incoming administration won’t see DACA recipients as a priority.”

Mayors Group Calls For Immigration Reform, Protection For Dreamers. [The Hill](#) (1/18, Bernal, 1.25M) reports the United States Conference of Mayors (USCM) on Wednesday called on Congress “to move quickly on immigration reform and to immediately protect young immigrants from deportation.” The Hill says the USCM passed an emergency resolution seeking comprehensive immigration reform, submitted by LA Mayor Eric Garcetti, Anaheim Mayor Tom Tait, Providence Mayor Jorge Elorza, and Seattle Mayor Ed Murray. They also urged that the protection of Dreamers from deportation be made a priority by the incoming Trump Administration.

Speaking to reporters, Garcetti said, “This resolution says to the American people that regardless of party or of ideology, America’s mayors are united in the belief that we must and we can fix our broken immigration system,” the [Los Angeles Times](#) (1/18, 4.52M) reports. Regarding Dreamers, he also said, “These are people we can point to in our communities as aiding our economies, as starting our businesses, as making our streets safer. My main point is, let’s not go backwards.”

The [Seattle Times](#) (1/18, Beekman, 1.05M) adds the resolution “calls on Congress and Trump to continue programs that give temporary status to Dreamers and to the relatives of people serving in the military.”

Afghan Translators Visa Program Backlog Leaves Many In Fear For Their Lives. The [Huffington Post](#) (1/18, Blanchard, 237K) reports that Congress’ renewal of the visa program for Afghans who provided assistance to US forces occurred with “far fewer openings than [in] previous years,” which it says is leaving “thousands of Afghans living in fear as they wait out the backlog.” The approval of only an additional 1,500 visas for the program, the Post says, “is likely to exacerbate a growing backlog to the program, which is still accepting new applications.” It is this backlog that has also left many Afghan applicants and their families “with a long wait for visas – often between two to six years. During this time, they are extremely vulnerable to being targeted by insurgents.”

IMMIGRATION

Feds Answer Questions Regarding Policy Change On Cuban Migrants. The [Miami Herald](#) (1/18, Gámez Torres, 856K) reports the White House and the Department of Homeland Security have answered questions regarding the end of the “wet foot, dry foot” policy as well as the Cuban Medical Professional Parole program (CMPP). In response to the question of whether Cuban nationals seeking entry at the southern border will be sent back, DHS said, “Like migrants from other countries, Cuban nationals will be

subject to expedited removal. The Department of Homeland Security will take steps to repatriate Cubans who are ordered removed and have exhausted their claims for relief.” The Herald says DHS indicated that doctors who arrived in the US after the policy was implemented and were approved under the prior policy receive an annotated stamp that reads: “It is not a visa. The carrier has received parole by USCIS under the CMPP.”

Chicago Tribune: Trump Should Allow Cuba Policy Shift “To Stand.” The [Chicago Tribune](#) (1/18, 2.54M) editorializes that it is “hard to predict” whether President-elect Trump will allow President Obama’s policy shift on Cuba to stand. The shift, the Tribune says, “will create hardship for some,” but whether Trump will be swayed by the stories of Cubans stranded at the Mexican border and separated from their families is unclear, given that he has yet to articulate a Cuba policy. The Tribune asserts, however, that he should allow the shift to remain as he formulates his policy, and “he should think about the fallout if normalization with Cuba unravels. Five decades of embargo and diplomatic dead air have not brought Cuba any closer to democratic and human rights reform. There should be no turning back.”

Policy Analyst: End Of “Wet Foot, Dry Foot” Makes It Harder For Cubans “To Seek Their Freedom.” Cato Institute’s Center for Global Liberty and Prosperity immigration policy analyst Alex Nowrasteh writes in the [Huffington Post](#) (1/18, Nowrasteh, 237K) that while ending the “wet foot, dry foot” policy and “diverting Cubans into the backlogged asylum system” and allowing them to seek green cards under the Cuban Adjustment Act is “not the end of the world for Cubans,” it does make “the process less predictable, more intimidating, and can result in some Cuban asylum seekers waiting in detention facilities or treated as criminals for fleeing Communism.” Nowrasteh says, “It’s a shame that one of President Obama’s last moves in the Oval Office dims our beacon of liberty and makes it more difficult for Cubans to seek their freedom.”

Haley “Repudiates” Muslim Registry Idea Under Trump. [The Hill](#) (1/18, Kamisar, 1.25M) reports President-elect Trump’s pick for UN ambassador Nikki Haley at her Wednesday confirmation hearing “repudiated the idea of a registry for Muslim immigrants or Muslim Americans.” When asked about Trump’s campaign comments about such a registry, she noted he no longer supports the idea, saying, “His administration and I don’t think there should be any registry based on religion. ... What we do need to do is know which countries are a threat and those are the ones we need to watch and be careful and vet.”

Fed Dallas President Kaplan Says Immigration Makes US Stronger. [Bloomberg News](#) (1/18, Matthews,

2.41M) reports Federal Reserve Bank of Dallas President Robert Kaplan “said trade with Mexico protects U.S. jobs and immigration is key to the country’s long-term health.” Kaplan, who made his remarks Wednesday in Dallas, “spelled out why their southern neighbor was already deeply integrated within the U.S. economy.” Kaplan also said one of the nation’s greatest assets is “we have been historically receptive to immigrants. Immigrants and their children make up over half of the growth in the labor force in the United States in the last 20 years.”

PRI: More Mexicans Leaving US For Mexico.

[Public Radio International](#) (1/18, 36K) reports on an increasing trend of Mexicans leaving the US to return to Mexico. PRI says the trend started around the 2007-2008 financial crisis and has since increased. PRI highlights the story of Mario Ramos and his wife Cristina Vargas who left Memphis after 12 years and returned to Mexico in 2015. Ramos and Vargas said politics did not influence their decision, but rather they returned to Mexico for fear of losing a house and parcels of land they owned there. A survey also found that “61 percent of departing Mexicans said they had returned to their home country to reunite with family or start a new family.”

US COAST GUARD

Coast Guardsman Attending Training Course Dies.

The [Newport News \(VA\) Daily Press](#) (1/18, Subscription Publication, 182K) reports Coast Guardsman Lt. junior grade Devin Hepner died Monday morning after being “found unresponsive in his barracks room.” He was “attending a training course at the Coast Guard Training Center in Yorktown.”

Coast Guard To Install Additional Radio Activation Switches At Maine Lighthouses.

The [Bangor \(ME\) Daily News](#) (1/18, 165K) reports the Coast Guard is planning on installing seven additional Mariner Radio Activated Sound Signals at lighthouses along the Maine coast in order to “reduce negative effects of continuous foghorns on area wildlife...and residents of the areas.” The Coast Guard replaced 17 traditional fog detectors with the mariner-activated fog detectors along the Maine coast last year. The new signal devices “allow mariners to activate lighthouse sound signals on-demand with a marine radio, Lt. David Bourbeau, spokesman for Coast Guard Sector Northern New England in South Portland, said in a release.” Commander of Coast Guard Sector Northern New England said, “This change will allow us to reduce our overall footprint by decreasing the required number of solar panels and lead acid batteries onsite when compared to the current

configuration.” The Daily News says the public will have an opportunity to comment prior to the installation.

SECRET SERVICE

DisruptJ20 Protest Group Vows To Disrupt Inauguration Events.

[Reuters](#) (1/18, Johnson, Simpson) reports the leaders of the DisruptJ20 protest group “vowed on Wednesday to disrupt his inauguration this week by blocking public access to the event.” The group “said it will send groups of demonstrators to the dozen entrances to the grassy National Mall where hundreds of thousands of people are expected to gather to watch” the inauguration.

Trump Inauguration Parties Likely To “Be Markedly Muted” Compared To His Predecessors’.

The [Washington Post](#) (1/18, Judkis, 11.43M) reports that while “it’s hard to predict the size of the crowds that will greet President-elect Donald Trump at his public events this week, it seems increasingly clear that the after-hours revelry will be markedly muted. Not only is Trump hosting only three official balls – far fewer than his predecessors at their first inaugurals – but the spillover festivities appear smaller and fewer.” The Post adds, “Far fewer big-name celebrities are headed to town. And while many events are reportedly sold out, others are still looking to fill their rooms.”

NYTimes Examines How Size Of Crowds At The Capitol Have Been Counted Over The Years.

The [New York Times](#) (1/18, Wallace, Subscription Publication, 13.9M) offers a look at “how the tools for counting” the size of crowds that have “descended on Washington to witness, celebrate and protest since the cornerstone was laid on the Capitol building in 1793” have evolved “over the last 150 years.”

Man Appears To Have Set Himself On Fire Outside Trump Hotel In DC.

The [Washington Post](#) (1/17, Weil, Williams, 11.43M) reported that a man suffered severe burns on Tuesday night “after apparently setting himself on fire in the street outside the Trump Hotel on Pennsylvania Avenue NW, according to a public safety source with knowledge of the incident,” who “said that arriving rescue personnel found a 45-year-old man who had been using a lighter and an accelerant. No motivation could be learned. However, a construction worker in the area said he saw a man surrounded by flames, uttering the name of President-elect Trump in what appeared to be an angry manner.” The Post added, “The man was taken to a hospital with what were described as third-degree burns on about 10 percent of his body.”

Florida Man Charged With Threatening To Kill Trump.

The [Washington Times](#) (1/18, Noble, 272K) reports, “A Florida man faces criminal charges for using his

Twitter account to make a threat to kill President-elect Donald Trump, according to the Miami Beach Police Department. Dominic Joseph Puopolo, 51, was arrested after posting a video on Twitter in which he said, "This is the 16th of January 2017, I will be at the review/inauguration and I will kill President Trump, President elect Trump today." Puopolo, "who is listed as homeless on the report, was arrested Tuesday as he left a Miami Beach Subway restaurant," and "was being held without bond on a charge of threatening harm against a public servant."

Additional coverage is provided by [TMZ](#) (1/18, 3.28M) and [Inside Edition](#) (1/19, 391K).

Continuing Coverage: Secret Service Settles Discrimination Case.

In continuing coverage, [CNN](#) (1/18, Meier, 29.79M) reports the Secret Service "has agreed pay \$24 million to settle a racial discrimination case brought on by eight African-American Secret Service agents who alleged that the federal agency denied them job opportunities because of their race, according to court documents." CNN quotes Secretary Johnson, from his statement, as saying, "Had the matter gone to trial, it would have required that we re-live things long past, just at a time when the Secret Service is on the mend. Under Joe Clancy's leadership, the Secret Service has turned the corner, and today's settlement is part of that."

The [Christian Science Monitor](#) (1/18, 387K) reports the settlement is a "small but meaningful step toward reforming serious problems in [the agency's] operations." The Monitor adds that the "settlement marks a willingness to turn over a new leaf, and to guard against further discrimination."

The [Atlanta Journal-Constitution](#) (1/18, 1.41M) profiles former Secret Service agent Ray Moore, who filed the lawsuit after being passed over for a promotion in 1999. He said, "I just wanted to effect change, and I did."

[NPR](#) (1/18, 1.92M) reports similarly on the settlement.

Pence Motorcade Injures DC Police Officer.

[WRC-TV](#) Washington (1/18, 453K) reports on its website that Vice President-elect Pence's motorcade "struck and injured a D.C. police reserve officer Wednesday afternoon, according to the U.S. Secret Service." The officer was struck while conducting traffic control. He has already been released from the hospital.

NATIONAL PROTECTION AND PROGRAMS

Protective Security Service Officer Accidentally Shoots Self In Leg. The [Washington Post](#) (1/18, Hermann, 11.43M) reports a Protective Security Service

officer "accidentally shot himself in the leg Wednesday afternoon while in a traffic control booth on Pennsylvania Avenue." The officer "was reported in good condition at a hospital." He is a "member of the Protective Security Service, which guards government buildings under a contract with the Federal Protective Service, under the Department of Homeland Security."

Minnesota Lawmakers To Consider Real ID Compliance Legislation.

The [AP](#) (1/18) reports Minnesota state Sen. Warren Limmer, who "led the charge on the 2009 ban" of Real ID in the state, "said Wednesday he won't block a vote on the measure, potentially clearing the way for the state to comply with the Real ID Act and avoid domestic travel disruptions starting next year." Limmer "said Wednesday he still opposes the federal law but that he would let a proposal to upgrade Minnesota IDs come to a vote in the Senate Judiciary Committee he chairs."

The [St. Paul \(MN\) Pioneer Press](#) (1/18, 460K) reports a state "House measure to change Minnesota licenses so that they will be accepted by the federal government by the 2018 deadline won a narrow 12-11 vote in a House committee Wednesday." The House bill would "create two tracks for new Minnesota driver's licenses," one that is compliant with Real ID and one that is not. The issuance of the non-compliant license "would allow Minnesotans who chose to do so to opt out of the extra security measures needed for the federally approved Real ID license."

South Carolina Visitors To Fort Bragg May Use Licenses Until June.

The [Fayetteville \(NC\) Observer](#) (1/18, 142K) reports, "Fort Bragg visitors from South Carolina will be able to continue to use their state driver's licenses to enter post, at least for a few more months." South Carolina was "included earlier this month on a list of states not in compliance with the REAL ID Act, a federal law designed to help officials combat fake identification." South Carolina, "along with Alaska, California, Oklahoma, Oregon and Virginia, now have until June 6 to comply or risk running afoul of" Real ID. The [AP](#) (1/18) cites the Observer's reporting.

Stop The Bleed Program Introduced In Des Moines. The [AP](#) (1/18) reports, in brief, that DHS' Stop the Bleed program is being introduced in Des Moines.

TERRORISM INVESTIGATIONS

Justices Appear To Favor Bush Administration Officials In 9/11 Detainee Case. [USA Today](#) (1/18, Wolf, 5.28M) reports that six Supreme Court justices "were forced Wednesday to relive the calamitous months following the Sept. 11 terrorist attacks, and most seemed inclined to

forgive Bush administration officials for the harsh treatment of Middle Eastern men later found to be innocent.” USA adds that “arguing its last case before the high court, President Obama’s Justice Department said former attorney general John Ashcroft and others should not be held personally liable for decisions made in the climate of fear that followed the attacks in New York and Washington,” and “that appeared to be a winning argument against claims brought by six Muslim non-citizens who were among hundreds jailed in extremely harsh conditions because they fit the same racial and religious profile of the 9/11 hijackers.”

The [Washington Post](#) (1/18, Marimow, Hauslohner, 11.43M) reports that the “long-running case dates to the months after the attacks, when hundreds of Arab and South Asian men – many of them Muslim – were arrested and detained as part of a nationwide terrorism probe.” Six plaintiffs “say they were beaten, strip-searched and treated as terrorism suspects because of their religion and ethnicity,” and the men, “who all lacked lawful immigration status, were held for months in highly restrictive conditions in a federal detention center in Brooklyn, but none were found to have any connection to terrorism.” The Post adds that “two of the court’s liberal justices, Ruth Bader Ginsburg and Stephen G. Breyer, seemed particularly troubled during oral arguments Wednesday about their treatment and the length of their incarceration, even after government officials knew the men had no ties to terrorism months after the September attacks.”

[Reuters](#) (1/18, Hurley) reports during the arguments, Chief Justice Roberts “expressed concern that permitting such lawsuits against senior U.S. officials would become ‘a way of challenging national policy’ through litigation seeking monetary damages against the individuals who implemented the policy.”

The [AP](#) (1/18, Sherman) reports Justice Department lawyer Ian Gershengorn “said the court should not subject the former heads of the Justice Department and FBI to a lawsuit where they could be personally liable for paying money to the plaintiffs for actions they took following the Sept. 11 attacks ‘to avoid the inadvertent or premature release of a dangerous terrorist.’” He said Ashcroft, at the time, was “trying to sort through how to respond to a very difficult situation.” [The Hill](#) (1/18, Wheeler, 1.25M) reports Gershengorn additionally “argued that his clients can’t be sued because there’s no proof they ordered the detainees to be abused.”

The [Huffington Post](#) (1/18, 237K) reports Gershengorn “argued that [the] list of suspects were ‘facially valid constitutional policies,’ and that a group of former detainees who sued former...officials over their deployment have no legal recourse against them in the courts.” The Post adds that the Justice’s decision in the case could have “profound implications for the incoming administration, whose soon-to-be chief executive clinched the presidency on promises that he’d mass-deport millions of undocumented immigrants, ban

Muslims from entering the country and bring back torture for terrorism suspects.”

Plaintiff Ahmer Abbasi writes in an op-ed for the [New York Daily News](#) that he was “was swept up with lots of other Muslim, Arab and South Asian men, held in immigration detention for months in isolation, beaten and harassed” after the September 11 attacks. Abbasi claims that he “later learned that these sweeps, and the targeting of men like me, were ordered by officials at the highest levels of the Bush administration.” He says his two months spent in detention were the “worst of my life.” He opines that the “truth was, I was arrested, imprisoned, isolated and abused because officials, including former Attorney General John Ashcroft and FBI Director Robert Mueller, thought I was suspicious and dangerous based on nothing more than my race and my faith.”

FBI Probing Second Wave Of Bomb Threats To Jewish Community Centers. [NBC Nightly News](#)

(1/18, story 8, 0:15, Holt, 16.61M) reported that the FBI is investigating “a round of bomb threats at dozens of Jewish community centers across the country,” the “second rash of scares in as many weeks.” Several centers “were evacuated as a precaution,” and “all of the calls were found to be hoaxes.”

[Reuters](#) (1/18, Ingram) reports that 27 Jewish community centers in 17 states “reported receiving false telephone bomb threats on Wednesday, prompting evacuations and an FBI probe into the second wave of hoax attacks to target American Jewish facilities this month.” The JCC Association of North America “said the threatened organizations were working with police and many had resumed operations after no bombs were found nor injuries reported, as was the case after the earlier series of threats on Jan. 9.” The FBI said in a statement that it and the Justice Department “are investigating possible civil rights violations in connection with threats.”

Pence: Americans’ Safety, Security Is Trump’s Top Priority. [Vice President-elect Pence was asked on Fox News’ Special Report](#)

(1/18, 1.53M) about a New York Times report which said that Obama Administration officials do not know if incoming Trump Administration officials have read the briefing papers they have provided on the threat “the new team could face in the first weeks in office.” Pence said, “I can assure you that the information flow has been very positive. Our team – whether it is our national security teams, whether it be our incoming nominees leading the CIA or department of national intelligence have all been working very closely with the administration. The safety and security of the American people is the top priority of any President, including our President-elect.”

Trump Expected To Seek Reform Of Intelligence Community. The [Washington Times](#) (1/18, Gertz, 272K) reports President-elect Donald Trump intends “to reform the heavily bureaucratized and, to some critics, politicized U.S. intelligence community.” And is even considering “plans to do away with the director of national intelligence.” That might mean a return “to the old system of having a director of central intelligence as a nominal chief.”

Obama Administration Issues New Rules Governing CIA Collection Of Information About Americans. The [New York Times](#) (1/18, Savage, Subscription Publication, 13.9M) reports the Obama Administration has just “overhauled and lifted a veil of secrecy from rules governing the C.I.A.’s power to gather and use information about Americans.” The rules had not been updated since the Reagan Administration. In addition to updating the rules, the Administration “is making all 41 pages of the rules public.” CIA Director John O. Brennan approved them on January 10, and Attorney General Loretta E. Lynch “signed them on Tuesday.”

In Mali, Truck Bomb Kills 60, Injures More Than 100 At Army Base. The [Washington Post](#) (1/18, Sieff, 11.43M) reports an attack in Mali by “a suicide truck bomb killed at least 60 people” including “soldiers, members of pro-government forces and fighters from autonomous armed groups.” The attack was against a camp housing “600 men from two pro-government militias and the Malian army.” Malian President Ibrahim Boubacar Keita “declared three days of national mourning.” The [AP](#) (1/18) reports the attack took place about 9:00 a.m. at the Joint Operational Mechanism base in Gao.

[Reuters](#) (1/18, Ag Anara) reports Al Qaeda in the Islamic Maghreb issued a statement Wednesday saying that the attack in Northern Mali, which killed up to 60 people and injured more than 100, was in retaliation for cooperation with France. President Keita, speaking on television Wednesday, said, “We will fight you. We will defeat you. You will not have the last word.” AQIM said the attack was conducted by al Mourabitoun, an affiliated group.

Guantanamo Bay Detention Center Remains Open As Obama Exits Stage. The [Washington Times](#) (1/18, Dinan, Miller, 272K) reports President Obama has “come ever so close to his goal” of closing the detention center at Guantanamo Bay, Cuba, as “just 45 detainees remain, down from the 242” at the beginning of his term. The Times points out that at the end of 2008, Sen. John McCain (R-AZ) and President Bush both favored closing the center, yet, neither Democrats nor Republicans in the Congress shared that view. The article offers a history of the attempts to close it by the Administration.

Widow Of Orlando Nightclub Gunman Pleads Not Guilty. The [AP](#) (1/18) reports that Noor Salman, the widow of Orlando nightclub shooter Omar Mateen, pleaded not guilty Wednesday to charges that she aided and abetted her husband’s support of terrorism and hindered the investigation into the deadly attack. “Noor Salman, 30, entered her plea in an Oakland courtroom two days after she was taken into custody at the home she shared with her mother in suburban San Francisco,” the AP says. Federal prosecutors say Salman knew of her husband’s plot and lied to FBI agents following the attack. [Reuters](#) (1/18, Todd) reports Salman faces up to life imprisonment on the charges against her.

Suspect Arrested For Allegedly Communicating Fake Bomb Threat To Flight Crew. The [Denver Post](#) (1/18, Mitchell, 778K) reports “a 20-year-old man, who has been arrested for allegedly falsely claiming he found a letter in an airplane bathroom that indicated a bomb was on [a] United Airlines flight, faces a potential penalty of 10 years in federal prison and \$250,000 fine.” FBI agents on Monday arrested Cameron E. Korth on charges of maliciously conveying false information. He was set to appear in court yesterday. The note Korth claimed to have found in the bathroom said there was a bomb on the plane and the pilots should not attempt to land. The crew notified the FBI. No explosives were found when the plane landed in Denver. “The FBI determined that Korth wrote the note in his seat on paper he found jammed in the seat and took it into a bathroom,” the Post says.

Algerian Gitmo Detainee’s Transfer Appeal Denied. The Associate Press provided three different reports on news that an Algerian Guantanamo Bay detainee lost his last minute legal appeal to be released. The [AP](#) (1/18) reports US District Judge Rosemary Collyer “declined to intervene in a Defense Department decision not to repatriate Sufyan Barhoumi, 43, in the final days of the Obama administration.” Barhoumi’s repatriation was approved by the government review board in August. The [AP](#) (1/18) says Barhoumi’s legal team argues “that there is no longer any justification for holding [him] given the board’s decision, which found that both countries could adequately ensure neither” Barhoumi nor a Moroccan prisoner in a similar position “posed a threat in the future.” However, another [AP](#) (1/18) piece says Defense Secretary Carter failed to give final approval and issue a 30-day notice to Congress of the prisoner’s impending release, which is required by law. Barhoumi’s attorney Shane Kadidal “said he would probably not appeal with time running out before the inauguration.”

[The Guardian \(UK\)](#) (1/18, Ackerman, 4.07M) says that two “knowledgeable US officials” expect a final round of

transfers from the prison before Obama leaves office. The article says three or four prisoners could be released, which would mean Obama “will leave office with either 41 or 42 men still detained at Guantánamo...as his plan to close the infamous detention facility falls short.”

Judge Rules DOD Must Release Abu Ghraib Photos. [Reuters](#) (1/18, Stempel) reports that US District Judge Alvin Hellerstein in New York ruled on Wednesday that the Defense Department “must release a cache of photos showing how Army personnel treated detainees at the Abu Ghraib prison and other sites in Iraq and Afghanistan.” Judge Hellerstein “said the release was proper because departing Defense Secretary Ash Carter failed to show why publishing the photos would endanger Americans deployed outside the United States.” Reuters adds that Judge Hellerstein’s decision “is a victory for the American Civil Liberties Union and other civil and veterans rights groups whose lawsuit seeking the photos under the federal Freedom of Information Act began in 2004.”

CYBER NEWS

DHS Releases Updated National Cyber Incident Response Plan. The [Federal Times](#) (1/18, 117K) reports, “Months after it requested input from the private sector on how to improve its cybersecurity response and coordination,” DHS “released an updated version of the National Cyber Incident Response Plan on Jan. 18” that “outlines the roles and responsibilities of federal, state, local and even private stakeholders in the wake of a cyberattack.” Secretary Johnson “said in a statement that the completion of the 180-day review of the plan will help strengthen the nation’s resolve to combat future cyber breaches.”

Senate Armed Services Committee Creates Cybersecurity Standing Subcommittee. [Florida Politics](#) (1/18) reports the US Armed Services Committee “has created a new standing subcommittee on cybersecurity and U.S. Sen. Bill Nelson will be the ranking Democrat to help lead it.” Senator John McCain “announced the panel’s creation Wednesday afternoon and appointed U.S. Sen. Mike Rounds...as chairman.” Florida Politics says, “Little else is determined at this point,” adding that “the rest of the committee will be filled out and its purposes and schedule set as Rounds and Nelson work that out.”

State Officials Felt “Blindsided” By Decision To Designate Elections Systems As Critical Infrastructure. [CyberScoop](#) (1/18) reports, “The state officials who actually run U.S. elections have written to the Department of Homeland Security to question the recent

designation of elections systems as ‘critical infrastructure,’ saying they don’t know what the move means and fretting it will interfere with efforts to secure voting machinery, both online and in the physical world.” State officials “told CyberScoop they felt blindsided by the decision, and some plan to ask the incoming administration of President-elect Donald Trump to repeal the move.”

Chaffetz Requests Information On “Unauthorized Scans” Of Georgia Secretary Of State Firewall. [Federal Computer Week](#) (1/18, 263K) reports House Oversight Committee Chairman Jason Chaffetz “wants a fuller accounting from the Department of Homeland Security about complaints of the agency ‘rattling of doorknobs’ on the state of Georgia’s network firewall.” Chaffetz “sent letters on Jan. 11 to DHS Secretary Jeh Johnson and DHS Inspector General John Roth asking about ‘unauthorized scans’ and ‘unsuccessful attempts to penetrate’ the Georgia Secretary of State’s firewall from last February into November’s election season.” Chaffetz, in his letter to Roth, “requested the IG open an investigation into DHS’ activities with the Georgia system,” and “requested all of the DHS secretary’s correspondence with” Georgia Secretary of State Brian Kemp.

Cyber Expert Highlights Animal-Caused Outages To Bring Perspective To Cyber Debate. The [Washington Post](#) (1/18, Wootson, 11.43M) reports that “as the nation is at perhaps its most apoplectic about what, exactly, Russian computers are doing to American ones,” cybersecurity expert Cris Thomas “has been tracking reports of ‘cyberwar operations’ by animals in the English-speaking world.” The Post adds, “Squirrels are the leading, and possibly cutest, attackers. They’ve been responsible for 879 successful attacks.” Thomas is quoted saying at a hacker convention, “If these numbers are accurate, squirrels just aren’t winning the cyberwar, they’re crushing it.” The Post calls Thomas’s presentation “the latest iteration of his attempts to dispel myths about the threat of cyberwarfare and focus Americans’ fears where they should be rightly placed.”

[Wired](#) (1/18, 3.98M) says that CyberSquirrel1, Thomas’s compilation of animal-caused outages, “is more than just a satire, though; it’s Thomas’s attempt to put threats of cyberwar in perspective. Infrastructure security experts, though, aren’t entirely amused.”

GCHQ Establishes Cyber Contest For Teenage Girls. [Press Association \(UK\)](#) (1/18, Association) reports GCHQ’s new National Cyber Security Centre has set up a contest for teenage girls to “put their technology skills to the test in a competition that could unearth the cyber spies of the

future.” The contest is “part of efforts to inspire more women to join the fight against online crime.” GCHQ director Robert Hannigan is quoted saying, “The CyberFirst Girls Competition allows teams of young women a glimpse of this exciting world and provides a great opportunity to use new skills. My advice to all potential applicants would be: enjoy the experience and I look forward to meeting some of you.” [BBC News \(UK\)](#) (1/18, 2.39M) reports similarly.

White House Cybersecurity Coordinator Defends Obama’s Cyber Legacy. [Politico](#) (1/18, 2.46M) “Morning Cybersecurity” reports on an interview with White House cybersecurity coordinator Michael Daniel. Daniel “rejected Senate Armed Services Committee Chairman John McCain’s criticism that the Obama team never developed a comprehensive cyber strategy,” and also “defended the administration’s release of a report containing technical indicators about Russian hacking, which critics said would result in false positives because it included data not strictly linked to Kremlin operations.” Morning Cybersecurity adds that “it’s easy to forget that Daniel and his colleagues spearheaded a number of less flashy cyber developments in recent years.” Daniel is quoted saying, “Within the federal government, we have started a real culture change in terms of how agencies think about their information assets.”

Researchers Develop Protocol To Update Automobile Software To Reduce Hacking Vulnerability. The [Christian Science Monitor](#) (1/18, 387K) “Passcode” reports, “Unlike many cybersecurity experts, Justin Cappos doesn’t lay awake at night worrying about data breaches,” but “worries that malicious hackers may become more adept at remotely hijacking cars as they speed down the road.” Passcode says, “With automakers outfitting cars with computers that do everything from tighten seat belts to deploy airbags, experts worry that criminals could take advantage of vulnerabilities in those digital systems.” Cappos and his team at New York University, along with researchers from other institutions, “have set out to solve a key piece of the automotive cybersecurity puzzle: Remotely patching and updating old software.” Their “Uptane” protocol “aims to safely and securely update some of those millions of lines of code inside cars without drivers needing to return to dealerships.”

Sheth: Government Procurement, Budget Woes Lead To Insufficient Cybersecurity. Hitesh Sheth, chief executive officer of cybersecurity company Vectra Networks, writes in [The Hill](#) (1/18, 1.25M) “Congress Blog” that the “hacking tools identified by the FBI and Department of Homeland Security” as having been used by Russian-allied hackers to penetrate the Democratic National

Committee “are freely available on the internet. ... There is nothing special or even uniquely ‘Russian’ about them.” Sheth adds, “In the cybersecurity business we know the focus should be on our ineffective defense, rather than on finding the guilty country.” Sheth asserts, “Washington is a place where existing technology is aging, state-of-the-art solutions go undeployed, government security professionals live lives of frustration and bad guys meander unchallenged through federal networks.” Sheth places the blame on government procurement rules, but also on “our inability in recent years to budget for Federal operations on a regular, rational basis,” which “means the IT people in federal agencies can’t plan ahead for multi-year enhancements to the systems they must protect.”

Participants In Florida Cyber Contest Represent Eight-Fold Boost In Participation History. The [Pensacola \(FL\) News Journal](#) (1/18, 158K) reports, “When this year’s edition of CyberThon launches Friday at the National Naval Aviation Museum and National Flight Academy at Pensacola Naval Air Station, participants of the three-day cybersecurity event will represent a more than eightfold boost in the contest’s brief history.” Global Business Solutions CEO Randy Ramos “said the event’s growth signifies the rising prominence of cyber defense in Northwest Florida. He expects multiple economic players to continue collaborating in efforts such as CyberThon to nurture the region’s talent pipeline.” The News Journal adds, “In 2015, the event’s first year, 18 students participated, but Ramos expects about 146 students this weekend.”

Cyberweapons Deal Between Company, Mauritanian Government Devolves Into “International Incident.” In an approximately 4,500-word article, [Bloomberg News](#) (1/18, 2.41M) discusses Manish Kumar, a “globe-trotting cyberweapons dealer” whose company, Wolf Intelligence, offered services to the government of Mauritania. Bloomberg calls Kumar “no more than a competent coder,” but in the wake of Edward Snowden’s revelation of “the extent of National Security Agency espionage around the globe, most every country on earth wanted to develop its own mini-NSA.” Bloomberg also says the market for the most advanced “cyber arms” is “limited to the U.S. and the select few allies who can afford them,” while “the rest is dominated by lone-wolf savants and boutique companies whose interactions are characterized by what economists politely call a trust deficit.” Bloomberg goes on to detail Kumar’s background with finding and selling zero-day exploits, how he built his company, and how his deal with Mauritania “spiraled into an international incident.”

Ukrainian Utility: December Power Outage In Kiev Caused By Cyberattack.

[Reuters](#) (1/18, Polityuk, Vukmanovic, Jewkes) reports that a power blackout in Kiev last month “was caused by a cyber attack and investigators are trying to trace other potentially infected computers and establish the source of the breach, utility Ukrenergo told Reuters on Wednesday.” Preliminary findings from investigators hired by the utility “indicate that workstations and Supervisory Control and Data Acquisition (SCADA) systems, linked to the 330 kilowatt sub-station ‘North’, were influenced by external sources outside normal parameters, Ukrenergo said in comments emailed to Reuters.” Reuters adds, “The comments make no mention of which individual, group or country may have been behind the attack.”

Gallagher: Trump Favors “Aggressive” Cyber Posture, But Cyber Policies Unclear.

IT editor Sean Gallagher writes in [Ars Technica](#) (1/18, 1.61M), “Since Election Day, President-elect Donald Trump has taken an inordinate interest in some of the minutia of defense policy,” and “the same is true of the cyber realm.” Gallagher says Trump has pledged a “new focus on offensive ‘cyber’ capabilities.” While “that sort of aggressive posture is not a surprise...the policies that will drive the use of those physical and digital forces are still a bit murky.” Gallagher adds, “Given the difficulty of attribution...the kind of very attributable cyber force that US Cyber Command would wield as part of the Strategic Command would likely not act as much of a deterrent to low-level intrusions, espionage, and information operations.” Gallagher also says, “Nothing Trump or his proxies have said indicates any policy around shaping what ‘norms’ in the world connecting the digital to the physical should be.”

Poroshenko Calls For Global Response To Russian Hacking.

[Reuters](#) (1/18, Adler, Rao) reports Ukrainian President Petro Poroshenko called for “a worldwide effort to counter the threat of Russian cyber warfare” and urged the US to “be great again” by demonstrating leadership on issues such as global security. Poroshenko “played down speculation that Washington could backtrack on its support for Kiev,” noting that President-elect Trump “had said publicly he would stick to US obligations and there had been ‘promising’ statements by nominees to his cabinet.”

NATIONAL SECURITY NEWS

JCS Chairman Says Options In Fight Against ISIL Are Ready For New Administration.

The [Wall Street Journal](#) (1/18, Barnes, Subscription Publication,

6.37M) reports Joint Chiefs of Staff Chairman Marine Gen. Joseph Dunford in Brussels for meetings at NATO, said Wednesday that he has options prepared to present to James Mattis, nominee for secretary of defense, in the fight against ISIL. He also said that he has already met with President-elect Trump, Vice President-elect Pence, and other members of the incoming national security team. He said that the options include plans to prevent ISIL and other such groups from using Syria as a sanctuary from which to attack Iraq. Gen. Dunford did not provide further information on proposals. He did say that the transition team has been in discussions with the military for six weeks.

US Says Coalition Has Enough Local Arab Fighters To Move On Raqqa.

The [Wall Street Journal](#) (1/18, Lubold, Coker, Subscription Publication, 6.37M) reports US officials said that the coalition in Syria is now ready to move against ISIL in Raqqa, having recruited around 23,000 Arab men to fight. Yet, some in allied rebel groups doubt the numbers of Arab fighters the coalition claims. One local leader said the recruits were from the Syrian Democratic Forces and the numbers were just for public consumption. He estimated there were 1,200 fighters. Another rebel leader estimated 1,500 Arab fighters were available.

Russia Announces Joint Airstrikes With Turkey On ISIL Positions Around Al-Bab.

The [AP](#) (1/18, Isachenkov, El Deeb) reports Russian Lt. Gen. Sergei Rudskoi announced on Wednesday the first joint Russian-Turkish airstrikes around al-Bab in Northern Syria, “one of the few remaining IS strongholds” in the area. Rudskoi said a combined force of nine Russian and eight Turkish planes carried out strikes. The US-led coalition has also carried out airstrikes and reconnaissance in the area, according to coalition spokesman US Army Col. John Dorrian, speaking on Tuesday.

Turkey Suffers From War In Syria. The [Washington Post](#) (1/18, Cunningham, 11.43M) reports on the effects of the war in Syria on Turkey, which has suffered from terror attacks by both Kurdish separatists and ISIL supporters, while its soldiers are “dying in battles with the Islamic State in Syria.” The situation also has “strained” its relationship with the US, which is working with Kurdish forces in Syria. Turkey has now “softened its rhetoric” regarding President Assad and is working with Russia. Deputy Prime Minister Numan Kurtulmus said recently that he believes “our policy on Syria made big mistakes.”

Iraq Announces It Has Control Of Eastern Half Of Mosul.

The [New York Times](#) (1/18, Gladstone, Subscription Publication, 13.9M) reports Iraq announced

Wednesday that its forces have “control of the eastern half of Mosul.” Lt. Gen. Talib Shaghathi of the Iraqi Army said Wednesday “important lines and important areas are finished.” The [AP](#) (1/18, Salaheddin) reports that while the Iraqi government said the city’s eastern half was completely retaken, commanders on the ground said that some neighborhoods were not yet under control. [USA Today](#) (1/18, Michaels, 5.28M) reports US military spokesman Col. John Dorrian said eastern Mosul is “85% to 90% cleared of Islamic State militants.” He said that in western Mosul, the presence of up to 750,000 civilians “would probably have a tendency to complicate factors.” Still, he said, “We’re going to hammer the enemy with our air and artillery strikes to help facilitate their advance, and our advisers will be there to support them.”

The [Washington Post](#) (1/18, Holley, 11.43M) reports Iraq continues to face “the militants in western districts across the Tigris River.” Military officials said that ISIL retains control of “a handful of neighborhoods on the city’s eastern side” as well as the entire “western half.” Gen. Talib al-Kinani, who commands the counterterrorism forces that have provided the main force in Mosul, said that his forces had faced “more than 300 car bombs and many suicide bombers.” He also said that regaining the western side of the city would be “easier.”

WPost Analysis: Trump Faces Decisions About US Role In Afghanistan. The [Washington Post](#) (1/18, Jaffe, Ryan, 11.43M) reports the war in Afghanistan is in “a stalemate” with Afghan soldiers “fighting hard,” while “Taliban forces are taking territory,” though they have, so far, been unable to control “any major cities or towns.” President-elect Donald Trump, when speaking on the subject “has sounded as conflicted as his predecessor.” Trump has said that he “would stay in Afghanistan,” because “you have nuclear weapons in Pakistan,” and has spoken with Afghan President Ashraf Ghani. The Post says that Trump could provide “much more with relatively small increases in the size of the American force.” The Post points out that both retired Gen. James N. Mattis, and retired Lt. Gen. Michael T. Flynn both have extensive experience in Afghanistan.

Chinese President Continues Theme Of Global Cooperation At UN. [Reuters](#) (1/18, Miles, Nebahay) reports on a speech by Chinese President Xi Jinping at the United Nations in Geneva in which he said that China will have a “new model” of its relationship with the US. He also said, “Trade protectionism and self-isolation will benefit no one.” He also promised to “build a circle of friends across the whole world.” U.N. Secretary-General Antonio Guterres said Xi’s speech was “very reassuring”, but Sophie Richardson, China director at Human Rights Watch, said, “It is unfortunate that Chinese President Xi was given an obsequious red

carpet treatment at the U.N. today while NGOs with concerns about his dismal rights record were kept out.”

WPost: China Is Less Liberal Than Trump Administration Will Be. The [Washington Post](#) (1/18, 11.43M), in an editorial, calls Xi’s speech at the World Economic Forum “shrewd”, but also points out that China is “far less liberal or embracing of globalization than the Trump administration will be even if the worst fears of its critics come true.” The Post cites an American Chamber of Commerce in China report released Wednesday finding “81 percent of 462 surveyed companies said they felt less welcomed in the country than before.” In addition to economics, in China, “independent civil society has been virtually shut down, and critical journalists and academics silenced” while lawyers are “persecuted and imprisoned.”

Obama Warns Moving US Embassy To Jerusalem Could Be “Explosive.” [Reuters](#) (1/18, Mason, Rascoe) reports President Obama suggested Wednesday that moving the US Embassy to Jerusalem could have “explosive” results and “said he was worried that the prospects for a two-state solution to the Israeli-Palestinian conflict were waning.” Speaking to reporters at his last press conference as president, Obama said, “When sudden unilateral moves are made that speak to some of the core issues and sensitivities of either side, that can be explosive. That’s part of what we’ve tried to indicate to the incoming team in our transition process, is pay attention to this because this is...volatile stuff.” The [Washington Times](#) (1/18, Boyer, 272K) reports the President said it’s “right and appropriate for a new president to test old assumptions,” but “people feel deeply and passionately about this. The actions we take have enormous consequences and ramifications.” The [New York Post](#) (1/18, Fredericks, 3.82M) reports the President also expressed concern that the “moment may be passing” for a two-state solution, and that the “status quo is unsustainable.”

Cotton: US Should Move Embassy To Jerusalem. In an interview with [CNN’s Situation Room](#) (1/18, 554K), Sen. Tom Cotton said the US Embassy should be moved to Jerusalem. “The time is ripe,” he said, adding, “Israel has never been in a stronger position in the Middle East than they are now.”

Israel Deploys Upgraded Missile Defense System. [Reuters](#) (1/18, Heller) reports Israel’s “upgraded ballistic missile shield” became operational on Wednesday, in an extension of its capabilities “to outer space where incoming missiles can be safely destroyed.” The Defense Ministry said the US-funded Arrow 3 system would “significantly reduce the possibilities of ballistic missiles” hitting Israel.

Israeli Arab, Policeman Killed Amid Clashes Over Bedouin Village Demolition. The [Washington Post](#) (1/18,

Booth, Eglash, 11.43M) reports that in the predawn hours on Wednesday, “hundreds of Israeli police in riot gear, supported by helicopters, horses and armored personnel carriers, swept into” the Bedouin village of Umm al-Hiran to “demolish homes, barns and sheep pens deemed illegal.” A Bedouin schoolteacher “rammed his SUV into police, killing one officer” before being shot and killed by police. The [New York Times](#) (1/18, Kershner, Subscription Publication, 13.9M) reports that the “police version of the events was immediately disputed by the motorist’s relatives in the village...as well as human rights activists who had come to support the villagers. They insisted that he had plowed into the officers only after he was shot and lost control of the car.”

Power: UN Needs To “Push” Iran On Arms Embargo. [Reuters](#) (1/18, Nichols) reports Ambassador Power said Wednesday that the UN Security Council “needs to push Iran to abide by an arms embargo...amid UN concerns that Tehran has supplied weapons and missiles” to Hezbollah. In her last appearance at a public Security Council meeting, Power said that recognizing “progress on Iran’s nuclear issues should not distract this council from Iran’s other actions that continue to destabilize the Middle East.”

Biden, Stoltenberg Push Back Against Trump’s Claim NATO Is “Obsolete.” The [Wall Street Journal](#) (1/18, Troianovski, Subscription Publication, 6.37M) reports that Vice President Biden on Wednesday defended NATO and the EU, but did not mention Trump by name. Biden, speaking at the World Economic Forum in Davos, said cooperation between the US and Europe formed “the bedrock of the success the world enjoyed in the second half of the 20th century,” and “strengthening these values — values that served our community of nations so well for so long — is paramount to retaining the position of leadership that Western nations enjoy.”

The [Washington Post](#) (1/18, Birnbaum, 11.43M) reports NATO Secretary-General Jens Stoltenberg also “pushed hard” Wednesday against Trump’s comments that the alliance is “obsolete,” saying that it is constantly evolving to meet modern security threats, including terrorism. The Post says the “pushback in a roundtable with journalists — the first public response from the NATO leader since Trump slammed the organization in weekend comments — was the latest in an extraordinary public spat between the alliance that forms the backbone of Western security guarantees and the man who assumes command of the world’s biggest military superpower on Friday.” Nevertheless, Stoltenberg said he looked forward to working with Trump and that he was “absolutely certain that the United States will remain committed to security guarantees. There is strong bipartisan

support in the United States for the U.S. commitment to NATO.”

Pence: NATO To Remain Check On Russia. Vice President-elect Pence, [Politico](#) (1/18, Nussbaum, 2.46M) reports, said Wednesday that “NATO will remain a check on Russian power under the Trump Administration.” Days after President-elect Trump said the alliance was “obsolete,” Pence said, “That historic mission of NATO will go forward. I’m confident,” but added, “NATO needs to refocus its mission on confronting radical Islamic terrorism, the threat of ISIS, and the threat that that poses to member nations.”

McCain, Cotton Differ With Trump Over Stronger Russia Ties. Sen. John McCain told the [CBS Evening News](#) (1/18, story 5, 2:05, Pelley, 11.17M) that he hasn’t decided if he will support Tillerson’s nomination. McCain: “I am very concerned about someone who took a friendship award from Vladimir Putin, who...wants to restore the Russian empire.” When Scott Pelley later asked McCain what concerns he has for the Trump Administration going forward, the senator replied, “Primarily, Russia,” because Trump “continues to say things about how we can improve” relations with the Kremlin. McCain was also interviewed on [Fox News’ The O’Reilly Factor](#) (1/18, 767K), where he said he would be “deeply, deeply disappointed” if Trump lifts sanctions against Russia, adding, “so are all the people in the Baltic countries and in Ukraine and in Georgia, that right now are under the threat of military action by Vladimir Putin.”

When asked on [CNN’s Situation Room](#) (1/18, 554K) about President-elect Trump’s suggestion that he could ease sanctions against Russia once he takes office, Sen. Tom Cotton said he “would not ease the sanctions on Russia while they continue to occupy Crimea and” are engaged in the civil war in Ukraine.

Sources: FBI, Other Agencies Investigating Possible Kremlin Aid To Trump. [McClatchy](#) (1/18, Stone, Gordon, 74K) reports that according to “two people familiar with the matter,” the FBI and “five other law enforcement and intelligence agencies have collaborated for months in an investigation into Russian attempts to influence the November election, including whether money from the Kremlin covertly aided President-elect Donald Trump.” Officials at the FBI, CIA, NSA, Justice Department, the Treasury Department’s Financial Crimes Enforcement Network and representatives of the director of national intelligence are “examining how money may have moved from the Kremlin to covertly help Trump win,” the sources said. One of the allegations reportedly involves “whether a system for routinely paying thousands of Russian-American pensioners may have been used to pay some email hackers in the United States or to supply money to intermediaries who would then pay the hackers.”

Ex-British Ambassador To Russia Defends Providing Trump Dossier To McCain. The [CBS Evening News](#) (1/18, story 4, 2:25, Pelley, 11.17M) reported on Charlie D'Agata's interview with Andrew Wood, the former British Ambassador to Russia who in November gave Sen. John McCain the dossier that "contains unverified allegations of Mr. Trump's sexual behavior and potential bribes." Wood explained that he gave McCain the file "to say, 'this does exist,'" adding, "Anybody has reason to be concerned if they think the future President of the United States is somehow under Russian or any other tutelage." While Trump blasted the allegations as false, Wood said former MI6 agent Christopher Steele, who compiled the dossier, is "an honest professional. And nobody in his position would wish to make this sort of stuff up. It, after all, is potentially dangerous for him." Wood insists he isn't sure if the allegations are true, but he said the tactic of sexual entrapment by Russian intelligence services is "a very common practice."

Roger Stone Claims He Was Poisoned Over Knowledge Of Russian Hacking. The [Daily Mail](#) (1/18, 4.59M) reports "longtime Trump supporter" Roger Stone has "sensationally claimed he was poisoned by political enemies who wanted to kill him before he could 'debunk' their 'lie' that he knew Russians would hack the US election." According to Stone, doctors said a "mysterious and debilitating virus he was suddenly struck with in December was in fact polonium poisoning." He says the illness struck just as he was "accused by the Obama Administration of having prior knowledge Vladimir Putin was planning to meddle in the election."

Pence Downplays Concerns Over Trump Team's Foreign Policy Preparedness. With just two days until the inauguration, network and cable reporting centered on confirmation hearings for President-elect Trump's nominees. Coverage tended to focus on concerns about reports of a lack of a concrete foreign policy outlook for the incoming Administration, with reporting citing numerous examples in which Trump's nominees and fellow Republicans appear to differ with him on foreign policy issues. Appearing on [Fox News' Special Report](#) (1/18, 1.53M), Vice President-elect Pence was asked about a New York Times report that [said](#), "Nobody in the current Administration knows whether anyone in the [incoming Trump Administration] has read any" of the "nearly 1,000 pages of classified material" the Obama Administration has provided to Trump's transition team. In response, Pence said, "I can assure you that the information flow has been positive. Our team, our national security teams, our incoming nominees leading the CIA or Department of National Intelligence, have all been working very closely with the [Obama] Administration."

[CNN's Anderson Cooper 360](#) (1/18, 686K) said one of the headlines coming out of the confirmation hearings "is how few nominees have talked about major policy issues with Donald Trump." Jim Sciutto reported on [CNN's Situation Room](#) (1/18, 554K) that what "struck me" is that State Department officials say there has been "no big picture foreign policy discussions and the thing is that's been echoed by some of Trump's own national security appointees." For instance, Sciutto reported that Trump's nominee for US Ambassador to the UN, Nikki Haley, "said she has not had a deep dive discussion with the President-elect on, say, Russia, which is fairly remarkable considering the degree to which the intelligence community, the national security community views Russia as a threat." Wolf Blitzer [added](#) that Secretary of State-designate Rex Tillerson "also says...he hasn't really had a substantive major discussion with the President-elect on Russia."

Haass Warns Trump Against Making Sudden Foreign Policy Changes. Richard Haass, president of the Council on Foreign Relations, warns Trump in an op-ed for the [Wall Street Journal](#) (1/18, Subscription Publication, 6.37M) against making any sudden departures in foreign policy. He outlines three specific issues – moving the US Embassy in Israel, abandoning the Iran nuclear deal, and rejecting the long-held "One China" policy.

Russia Extends Snowden's Asylum. The [New York Times](#) (1/18, Kramer, Subscription Publication, 13.9M) reports that one day after President Obama commuted the sentence of Chelsea Manning, Russia on Wednesday said former NSA contractor Edward Snowden, "the other main source of secrets about United States surveillance in recent years," will be allowed to remain in the country for "a couple more years." According to the [Washington Post](#) (1/18, Roth, 11.43M), Snowden will now be able to stay in Russia "until 2020 — a time when he could theoretically apply for citizenship."

A [New York Times](#) (1/18, Subscription Publication, 13.9M) editorial says President Obama "did the right thing in granting clemency to Chelsea Manning," but showed "no similar mercy, so far, for...Snowden." The Times says that "like Ms. Manning, Mr. Snowden acted in the spirit of a whistle-blower," and his disclosures "led to significant debate and reforms." The Times argues that Snowden "should be offered at least a plea agreement that would allow him to return home."

Pence Says Assange Will Be Held Accountable If Extradited To US. Vice President-elect Pence was asked on [Fox News' Special Report](#) (1/18, 1.53M) if President-elect Trump's Justice Department will "actively and aggressively prosecute" Julian Assange if he allows himself to be extradited to the US. Pence said, "I think what the

President-elect has said is that the information that came out through WikiLeaks, which has never been questioned as having been real information, real emails that were verified, was useful to many Americans. That doesn't mean he agrees with or that we endorse the tactics or the actions of Julian Assange. If he is extradited to the United States of America or any jurisdiction, I am very confident that we would bring to bear the law on his actions and hold him accountable."

European Leaders Seek To Meet With Trump Before Putin. The [AP](#) (1/18, Pace, Grieshaber) reports that European leaders, "anxious over Donald Trump's unpredictability and kind words for the Kremlin, are scrambling to get face time with the new American president before he can meet with Russian President Vladimir Putin." According to the AP, "one leader has raised with Trump the prospect of a US-European Union summit early this year, and the head of NATO...is angling for an in-person meeting ahead of Putin as well." British Prime Minister Theresa May, meanwhile, is working to arrange a meeting in Washington "soon after Friday's inauguration."

Jammeh Faces Midnight Deadline To Step Down. The [AP](#) (1/18, Dione, Larson) reports that after more than two decades in power, Gambian President Yahya Jammeh "faced the prospect of a midnight military intervention by regional forces, as the man who once pledged to rule the West African nation for a billion years clung to power late Wednesday." A military commander with the regional bloc ECOWAS "announced that Jammeh had only hours to leave or face troops already positioning along Gambia's borders." Late Wednesday, witnesses reported Senegalese soldiers deploying along the border, and Nigeria "confirmed a warship was heading toward Gambia for 'training.'"

South Korean Court Rejects Arrest Of Samsung Heir In Corruption Case. The [Washington Post](#) (1/18, Fifield, 11.43M) reports that a South Korean court declined early Thursday to allow the arrest of Samsung's heir Lee Jae-yong for his alleged role in a corruption scandal in the country. The Post says the court's decision is "a shocking one for prosecutors," who accused Lee of "bribery, embezzlement and perjury, although the court decided only that Lee did not need to be detained, not that the case had no merit." The [New York Times](#) (1/18, Choe, Subscription Publication, 13.9M) says the court's decision is also "likely to anger many South Koreans" who have called for President Park Guen-hye's ouster and "the arrest of business tycoons on corruption charges."

Rights Groups Ask China To Free Tibetan Advocate. The [New York Times](#) (1/18, Wong, Subscription Publication, 13.9M) reports that international human rights groups are calling on China to "drop charges against a Tibetan entrepreneur and education advocate who was indicted" earlier this month for "inciting separatism." Tashi Wangchuk was detained "nearly one year ago after speaking to The New York Times for a documentary video and two articles on Tibetan education and culture."

Pakistani Jailed Doctor Thought To Have Helped CIA With Bin Laden Won't Be Freed. [Reuters](#) (1/18, Zahra-Malik) reports jailed Pakistani doctor Shakil Afridi, "hailed as a hero by U.S. officials," who believe he helped the CIA track down Osama bin Laden, "will be neither released nor handed to the United States," Pakistani Law Minister Zahid Hamid said, according to the Daily Times newspaper. Hamid is quoted as saying, "Afridi worked against the law and our national interest, and the Pakistan government has repeatedly been telling the United States that under our law he committed a crime." He reportedly added, "The law is taking its course and Afridi is having full opportunity of a fair trial."

NATIONAL NEWS

Media Analyses: Obama Sends Message To Trump During Final Press Conference. Media coverage of President Obama's final [news conference](#) on Wednesday is very heavy, including stories on all three network news broadcasts and extensive print and online reporting. The tone of the coverage is very positive toward Obama – but less so toward President-elect Trump. Among the issues highlighted were Obama's defense of the decision to commute the 35-year prison sentence of former military intelligence analyst Chelsea Manning, his praise for the press, and his claim that he wants to leave the limelight but will speak out in defense of what he described as the nations "core values" garner the most attention – a comment many reports cast as a warning to Trump that he will not be silent over the next four years.

[Politico](#) (1/18, Dove, 2.46M) said a "sober and cautious" Obama "presented a carefully constructed parting image" during "a performance that added to the long list of contrasts between the 44th and 45th presidents – one that will make even more jarring the shift that's happening at noon on Friday in front of the Capitol." [USA Today](#) (1/18, Korte, 5.28M) describes the President as "upbeat" during the news conference as he "carefully selected reporters from foreign and specialty news outlets, all but ensuring he would answer questions on immigration, the Middle East, gay rights and race relations." [The Hill](#) (1/18, Fabian, 1.25M) reported that

Obama “faced few, if any, pointed or confrontational questions from reporters.”

The [Los Angeles Times](#) (1/18, Parsons, 4.52M) reports that Obama’s comments “served as a message to his fellow Democrats,” many of whom “have talked in near-apocalyptic tones in recent weeks about the impending Trump administration.” Taking a “more measured” tone, Obama said, “I believe in this country. I believe in the American people. I believe that people are more good than bad. ... The only thing that’s the end of the world is the end of the world.” The [AP](#) (1/18, Benac) says Obama “insisted he’s not just tossing out reassuring platitudes about the nation’s future. It’s what he really believes.” He said, “This is not just a matter of no-drama Obama. ... It is true that behind closed doors I curse more than I do publicly. And sometimes I get mad and frustrated like everybody else does. But at my core, I think we’re going to be OK.” A brief report at the end of the [CBS Evening News](#) (1/18, story 12, 1:25, Pelley, 11.17M) also highlighted that comment, and [Vogue](#) (1/18, Codinha, 3.53M) said that the “emotional note...both soothed our fears and soared in its optimism and its belief in American exceptionalism.”

On its website, [People](#) (1/18, Sobieraj, 5.23M) said that when he was asked how his daughters felt about Trump’s victory, Obama said, “They were disappointed. ... They paid attention to what their mom said during the campaign and believed it because it’s consistent with what we’ve tried to teach them in our household, what I’ve tried to model as a father with their mom and what we’ve asked them to expect from future boyfriends or spouses.” Obama added, “They don’t mope. ... What makes me proudest about them is that they also don’t get cynical. They have not assumed that, because their side didn’t win or because some of the values they care about don’t seem as though they were vindicated, that somehow automatically, America had somehow rejected them or rejected their values.”

The [Washington Post](#) (1/18, Nakamura, 11.43M) reports that Obama defended “the final decisions he has made before leaving office,” and warned about “unintended consequences of policy shifts President-elect Donald Trump might trigger once he takes office.” According to [Roll Call](#) (1/18, Bennett, 63K), Obama “showed flashes of the optimistic candidate who toppled both Hillary Clinton and Sen. John McCain,” but “by the end of the session, his concerns about the next four years appear to show through.”

The [New Orleans Times-Picayune](#) (1/18, Rainey, 656K) saw a “pensive, almost wistful,” Obama who “steered clear of overtly reproaching” Trump, “although he did so in subtler ways.” [TIME](#) (1/18, Rhodan, 6.98M) similarly said Obama “subtly underscored his differences with Trump,” while [U.S. News & World Report](#) (1/18, Williams, 1.02M) called Obama’s news conference “another in a series of public warning shots to his untested successor.” On its website, [NPR](#) (1/18, Taylor,

1.92M) said the news conference “was one of both reflection and subtle rebuke toward” Trump, but added that Obama “did show some deference” toward the President-elect, “sidestepping a question about the more than five dozen Democrats in Congress who are boycotting the inauguration on Friday.”

A brief story from the [Washington Times](#) (1/18, Boyer, 272K) focuses on Obama’s claim that “he wants to stay out of the limelight for awhile,” but other reports highlight that Obama said he would speak out under certain circumstances. For example, the [New York Times](#) (1/18, Shear, Baker, Subscription Publication, 13.9M) says that Obama “made clear...that he would not go silent after leaving office this week.” According to the Times, Obama “has told friends that he did not intend to remain a mute bystander to the dismantling of important democratic ideals that he championed for eight years.” [Bloomberg Politics](#) (1/18, Talev, 201K) reports that while Obama said that he would “act to defend what he considers the nation’s ‘core values.’” Obama “said he would use his public platform as an ex-president to oppose any effort by the incoming Trump administration to ‘round up’ undocumented immigrants who arrived in the US as children.”

The Washington Post’s Eugene Robinson said on [MSNBC](#) (1/18, 232K) that Obama “listed not just things he cares about but things that he sees are beyond the pale of our democracy and that he has to speak out on, and I expect him to.” Robinson added that if the Trump Administration “moves in his view along any of these verboten paths, I think you’re going to hear him and I think he’ll be not just vocal, but pretty loud.” [Vox](#) (1/18, Lind, 1.15M) said Obama drew “a bright line: If President Trump does any of these things, Obama himself will be compelled to get back into the arena to defend them.”

In what the [New York Post](#) (1/18, Fredericks, 3.82M) says was a “not-so-veiled message” to Trump, Obama “pointedly talked about the news media’s vital role in a Democracy,” telling the press, “You’re not supposed to be sycophants, you’re supposed to be skeptics – cast a critical eye on folks who hold enormous power and make sure that we are accountable to the people who sent us here and you have done that.” [Variety](#) (1/18, Johnson, 492K) reported that Obama “called on the news media to cover the next administration ‘with the same tenacity that you showed us.’”

Michelle Kosinski said on [CNN’s Situation Room](#) (1/18, 554K), “This was absolutely a message to the incoming administration.” Also on [CNN’s Situation Room](#) (1/18, 554K), Dana Bash cited recent discussions “about moving the press, whether it’s the offices or the briefing room, into another facility on the grounds of the White House complex,” and said that Obama “made clear that’s not a good idea, but also more broadly that a free press, an adversarial press is one of the

cornerstones of American democracy and needs to continue to be that way.”

Lynn Sweet writes in the [Chicago Sun-Times](#) (1/18, 798K) that “a sentimental, reflective President Barack Obama” seemed “at peace with himself as he eagerly starts his next chapter on Friday.” His news conference was “heavy on the optimism that propelled him to this job in 2008.” Sweet added that when Obama “said he enjoyed working with the press,” she “took the salute more as jab to Trump, because he is so hostile to journalists.”

On [MSNBC's Hardball](#) (1/18, 713K), Kathleen Parker of the Washington Post said Obama “was being very artful in sending a message to Donald Trump because Donald Trump has been...calling us legitimate news organizations, fake news and alerted people that they're going to be losing their place in the press room at the White House. So in way without naming Trump, without, you know, without casting aspersions on him or anyone else, he was able to say, this is the reason we have a press, these are the things they need to do.” Juan Williams said on [Fox News' The Five](#) (1/18, 408K), “I thought President Obama was directly speaking to President-elect Trump about the press.” Eric Bolling was considerably less effusive on [Fox News' The Five](#) (1/18, 408K), saying that Obama “didn't really make any news. ... I think he was there as a final good-bye.”

Obama Defends Decision To Commute Manning's Sentence. Obama also defended his decision to commute Manning's sentence. [Reuters](#) (1/18, Mason, Volz) reports that Obama told reporters that “he felt it made sense to commute Manning's sentence because she went to trial and took responsibility for her crime.” Obama argued that Manning received a “very disproportionate” sentence compared to the sentences of other leakers. On [CNN's Situation Room](#) (1/18, 554K), Jim Sciutto reported that Obama's explanation is “very unlikely” to appease members of the intelligence and defense communities who are “extremely unhappy” with the commutation.

Meanwhile, Jonathan Karl reported on [ABC World News Tonight](#) (1/18, story 5, 2:30, Muir, 14.63M) that Obama's decision “was so controversial, his own Defense Secretary was against it, joining a chorus of Republican voices denouncing the move as damaging national security.” Catherine Herridge similarly reported on [Fox News' Special Report](#) (1/18, 1.53M) that Defense Secretary Carter “and top army leaders advised the President against the move because, a senior defense official said, the leaks likely contributed to the rise of violence and accelerated the Arab Spring.” Carter told the [AP](#) (1/18, Burns), “That was not my recommendation. ... I recommended against that, but the president has made his decision.”

Appearing on [Fox News' The O'Reilly Factor](#) (1/18, 767K), Senate Armed Services Committee Chairman John McCain said his reaction to Manning's commutation is “rage,

frustration and sorrow. Sorrow for the families of those individuals who identified in these leaks in Afghanistan that the Taliban went after and murdered. And rage because this President is basically endorsing a proposal that allows someone to go free who is responsible for the needless deaths of those people who are allies.”

On [Fox News' Special Report](#) (1/18, 1.53M), Vice President-elect Pence also took issue with Obama's decision, saying, “Private Manning is a traitor and should not have been turned into a martyr. ... The simple fact is that I disagree very strongly with the President's decision to commute Private Manning's sentence. We have to be so serious on the subject of protecting our nation's secrets, and so we will register strong disagreement with that, and our administration coming in, I can assure you – as you have heard the President-elect say again and again – is going to be committed to protecting our nation's secrets.”

[NBC Nightly News](#) (1/18, story 4, 2:20, Holt, 16.61M) briefly mentioned that while Obama defended commuting Manning's sentence, “critics argu[e] it sends a signal of weakness.” In a [USA Today](#) (1/18, 5.28M) op-ed, Scott Jennings, who served as Special Assistant to President George W. Bush from 2005-2007, calls the commutation “a fitting end to a failed presidency that leaves President-elect Donald Trump mess after mess to clean up on the world stage.”

In an editorial, [USA Today](#) (1/18, 5.28M) calls the Manning case “a thicket of contradictions and complexities,” and argues that if Obama “felt compelled to commute” Manning's sentence, “it would have been more appropriate to let Manning serve at least 10 years.” Doing so, USA Today argues, would have “struck a better balance between justice and respect for the intelligence community.”

Obama Says Voting Fraud Allegations Are “Fake News.” The [Huffington Post](#) (1/18, Levine, 237K) focused its coverage on Obama's comments on “efforts to make it more difficult to vote in the United States,” saying he called them “an extension of the legacy of slavery and Jim Crow laws.” Addressing “the notion that there were many incidences of voter fraud,” Obama said, “This whole notion of voting fraud, this is something that has constantly been disproved. This is fake news. The notion that there are a whole bunch of people who are going out there and are not eligible to vote and want to vote. ... We have the opposite problem. We have a whole bunch of people who are eligible to vote who don't vote. So the idea that we put in place a whole bunch of barriers to people voting doesn't making sense.”

Trump To Deliver “Very Personal” Inauguration Address. In a segment focusing on various aspects of President-elect Trump's inauguration, David Muir reported for [ABC World News Tonight](#) (1/18, story 4, 3:15, Muir, 14.63M)

that Trump “began writing his speech weeks ago, practicing on a podium with a prompter tonight. What kind of tone will he strike?” ABC’s Cecilia Vega added that “Trump today tweet[ed] a picture of himself in what he calls his winter White House, Mar-a-Lago, writing his speech, a bronzed eagle by his side. Unlike his sobering convention speech this summer, Friday’s themes: Uniting the country and America first. Aides calling it a very personal speech. It will be about 20 minutes long, Trump has been studying past inaugural addresses and practicing daily.”

On the [CBS Evening News](#) (1/18, story 2, 1:25, Pelley, 11.17M), Major Garrett also reported on Trump’s inaugural speech, saying “that slogan ‘Make America Great Again,’ the speech is going to be about defining what that means. Two big, broad goals for the country in pursuit of renewal. More economic growth, defined not just by more jobs but better paying jobs, especially in the manufacturing sector. And on security, reducing, if possible, the fear about terrorism with a concentrated effort to defeat ISIS. Broad goals defined in action words, and not a lot of soaring rhetoric, and as much as possible, nonpartisan and populist.”

At His Swearing-In, Trump To Use Both His Personal Bible And Lincoln Bible. The [New York Times](#) (1/18, McCann, Subscription Publication, 13.9M) reports that when Trump “takes the oath of office on Friday, he will do so with his hand on two Bibles: his own, and one used by Abraham Lincoln in 1861. Only one other president has used that Bible for the oath.” President Obama. The Times says “Trump’s personal Bible was given to him by his mother in 1955, two days before his ninth birthday, according to a statement from the inaugural committee.” The Lincoln Bible was used at Lincoln’s swearing in “at his first inaugural in 186” and “was not used again at an inauguration until the election of...Obama, who was sworn in on it in 2009 and again in 2013.”

Mattis Easily Clears Armed Services Committee. The [CBS Evening News](#) (1/18, story 6, 2:15, Pelley, 11.17M) and [Fox News Special Report](#) (1/18, 1.53M) both briefly reported that the Senate Armed Services Committee endorsed Mattis on Wednesday, with Sen. Kirsten Gillibrand the only dissenter in a 26-1 vote. The [Los Angeles Times](#) (1/18, Hennigan, 4.52M) says that Gillibrand “cited her concerns about maintaining civilian control of the military.” [Reuters](#) (1/18, Zengerle) and the [Washington Times](#) (1/18, Dinan, 272K) have brief reports.

Temporary Appointees To Take Posts On Friday At Noon. [Politico](#) (1/18, Restuccia, Cook, 2.46M) reports, “At 12:01 p.m. Friday, Donald Trump’s aides will deploy a team of temporary political appointees into federal agencies to begin laying the groundwork for the president-elect’s agenda while his nominees await Senate confirmation.” While the

transition team “has been building the so-called beachhead teams for months, they are taking on outsized importance because few of Trump’s nominees will be confirmed by the time he’s sworn in.”

WSJournal A1 Analysis: Nominees Challenging Status Quo. The [Wall Street Journal](#) (1/18, A1, Reinhard, Subscription Publication, 6.37M) writes on its front page that Trump’s Cabinet picks challenged the status quo on Wednesday, taking tough stances against China and federal environmental regulations. While some differed from Trump on specific issues, the Journal says they reflected his anti-establishment agenda.

Trump Says His Healthcare Plan Will Be Less Expensive Than ACA. The [New York Post](#) (1/18, Halper, Moore, 3.82M) reports President-elect Trump tried to assure skeptics during an interview on “Fox & Friends” that his ACA replacement plan would be less expensive than the ACA and would make sure “nobody is going to be dying on the streets.” He said, “We’re going to get private insurance companies to take care of a lot of the people that can afford it. They’re going to be able to have plans that are great plans.”

Pence: ACA Replacement Plan “Coming Together.” Vice President-elect Pence was asked on [Fox News’ Special Report](#) (1/18, 1.53M) about efforts to repeal and replace the ACA. Pence said, “The first priority will be keeping our promises, and the weight that Obamacare is placing on American families and businesses and our economy is enormous. ... The President-elect has made it clear to leaders in congress that he wants to repeal and replace concurrently on a dual track. We are working around the clock.” Pence added that the replacement plan is “coming together. ... Very simply, it’s going to be what the President-elect talked about in this election – allowing the American people to purchase health insurance across state lines, allowing the free market to meet the needs. We can have low cost health insurance in America by implementing free-market principles and implementing the kind of reforms in Medicaid that will allow underprivileged Americans to be able to take more control of their own healthcare.”

[ABC World News Tonight](#) (1/18, story 3, 1:25, Muir, 14.63M) showed Pence saying, “The President-elect has made it very clear to members of Congress that he wants to repeal and replace Obamacare at the same time. ... We want to repeal the individual mandates and the taxes and all those things that are putting such a hardship on American families today.” Asked whether the replacement would cover “every American”, Pence said, “The President-elect really believes in the power of the market place,” and “he talked consistently about his enthusiasm about allowing Americans to purchase

health insurance across state lines, the way we buy life insurance, the way we buy car insurance.”

Poll Finds Support For Doing Something, But Division Over What. The [AP](#) (1/18, Kellman, Swanson) reports on an Associated Press-NORC Center for Public Affairs Research poll of 1,017 US adults conducted December 14-19 finding “ample accord” on “the need to do something about health care in the United States” with nearly half of those polled calling it “a top issue”, but the poll also found “little agreement on what to do.”

Alexander Says ACA Repeal Should Not Happen Until Replacement Is Ready. The [Washington Times](#) (1/18, Howell, 272K) reports Senate Health Committee Chairman Lamar Alexander (R-TN) during a “courtesy hearing for Rep. Tom Price” as nominee to be secretary of health and human services, took the opportunity “to lay down his marker on repeal of Obamacare,” by “calling for simultaneous repeal and replace[ment] of the Affordable Care Act.” Alexander also explained that the hearing was a “courtesy” hearing as the HELP committee which he chairs does not vote on Price’s nomination, that will be done by the Senate Finance Committee.

[McClatchy](#) (1/18, Lightman, 74K) reports on an interview with Senate Majority Leader Mitch McConnell, in which he was asked about plans regarding the Affordable Care Act. He said, “That’s what the replacement will be about, and we’re not here to announce it today.” Asked about the measures success in reducing the number of uninsured, he said, “if the goal was to expand Medicaid, that could have been done alone,” but instead the ACA “tried to turn the private health insurance market into a regulated utility.”

Cuomo Says ACA Repeal Could Hurt New Yorkers. The [New York Post](#) (1/18, Fasick, Moore, 3.82M) reports New York Gov. Andrew Cuomo, after meeting with President-elect Trump Wednesday at Trump Tower, said, “We discussed how the ACA affects New York and the pitfalls of a repeal plan.” He said the repeal would cause around three million New Yorkers to lose insurance. Cuomo said, “it’s very important to protect the accomplishments that Obamacare also brought to us.”

NIH Director’s Response To Fungus In Medicine Vials Comes Under Criticism. The [Wall Street Journal](#) (1/18, A1, Burton, Subscription Publication, 6.37M) reports that fungus found in two vials of medicine in the NIH Clinical Center’s pharmacy has resulted in delays in medical trials and led to criticism of NIH Director Francis S. Collins for his management. Collins responded to the discovery by bringing in an outside team to review practices and shutting down labs that produce medications while they

updated their practices. Yet some in the NIH have accused him of overreacting, by adopting policies that have delayed patient treatment and research.

Senators Criticize DEA’s Enforcement Efforts Against Opioid Distributors. The [Washington Post](#) (1/18, Higham, Bernstein, 11.43M) reports seven US senators on Wednesday wrote to acting DEA administrator, Chuck Rosenberg, criticizing him and the agency for its response to questions they had sent regarding “enforcement actions against pharmaceutical companies” with respect to distribution of opioids. They had asked the DEA about the matter in October. The questions were sent after the Post reported that “beginning in 2013, DEA lawyers at headquarters started to delay and block enforcement efforts against large opioid distributors.” The senators who signed the letter are: Edward J. Markey (D-MA), Richard J. Durbin (D-IL), Joe Manchin III (D-WV), Amy Klobuchar (D-MN), Tammy Baldwin (D-WI), Richard Blumenthal (D-CT), and Bernie Sanders (I-VT).

Donors Announce \$500 Million For Organization To Combat Epidemics. The [New York Times](#) (1/18, McNeil, Subscription Publication, 13.9M) reports donors on Wednesday announced in Davos, Switzerland, they had “raised almost \$500 million” for the Coalition for Epidemic Preparedness Innovations. The coalition “will initially develop and stockpile vaccines against three known viral threats” and promote technological development to speed response to “new threats.” The Gates Foundation, Japan, Norway, and the UK’s Wellcome Trust are each contributing \$100 million to \$125 million, and contributions are also expected from Germany, India and the European Commission. In addition to donors, GlaxoSmithKline, Johnson & Johnson, Merck, Pfizer, Sanofi, and Takeda are “partners” as are the World Health Organization and Doctors Without Borders. The initial focus will be on developing vaccines “against Lassa fever, the Nipah virus and Middle East Respiratory Syndrome (MERS); and improving the latest DNA and RNA vaccine technology.”

Ryan, Bannon Collaborating On Tax Reform Plan. [The Hill](#) (1/18, Easley, Wong, 1.25M) reports that House Speaker Ryan and senior Adviser to President-elect Trump, Steve Bannon, “have embarked on a surprising collaboration, top aides say, sketching out a plan for tax reform that could be among the next president’s first major legislative achievements.” According to Trump senior adviser Kellyanne Conway, “Bannon and Ryan have been able to move beyond their bitter past and find compromise in conservative economic principles.” The “budding relationship has surprised and delighted members of Trump’s incoming

administration, which has otherwise been dogged by reports of infighting,” and “offers hope to Republicans worried that a feud between the two men would spell disaster for the party’s agenda.”

Haley Expresses Differences With Trump During Confirmation Hearing.

The [CBS Evening News](#) (1/18, story 3, 0:10, Pelley, 11.17M) reported briefly that UN Ambassador-designate Nikki Haley “distanced herself from the President-elect on Russia” on Wednesday, telling the Senate Foreign Relations Committee, “I don’t think we can trust them.” [Reuters](#) (1/18, Zengerle) says Haley “echoed” Trump’s “condemnation” of the UN, “but broke from the president-elect on some other policy issues, including Russia and NATO.”

[USA Today](#) (1/18, Durando, 5.28M) reports that Haley “vowed Wednesday to be a strong voice against Russia’s aggressive moves,” but “said the U.S. needs Moscow’s help to fight the Islamic State. ... On Israel, Haley said it was ‘a terrible mistake’ last month when the U.S. abstained on a U.N. Security Council resolution condemning Israeli settlements,” but said she backs a two-state solution.

The [Washington Post](#) (1/18, Gearan, Sullivan, 11.43M) say that Haley, “who had been critical of Trump as a candidate,” departed “sharply and sometimes awkwardly” from the President-elect, and “struggled at times to distance herself from some of Trump’s most controversial positions without openly contradicting him.” [McClatchy](#) (1/18, Bergengruen, Schofield, 74K) similarly writes that Haley “made it clear...that she disagrees with Donald Trump quite a bit regarding U.S. foreign policy.” The [Washington Times](#) (1/18, Miller, 272K) also reports on Haley’s hearing.

Ross: Renegotiating NAFTA Will Be Trump Administration’s First Trade Priority.

[Reuters](#) (1/18, Lawder) reports Commerce Secretary-designate Wilbur Ross told the Senate Commerce, Science, and Transportation Committee that renegotiating NAFTA “will be the Trump administration’s first trade priority.” Ross did not discuss President-elect Trump’s “threats to levy punitive tariffs on Chinese goods imported into the United States but said countries that fail to provide a fair trading field should be ‘severely punished.’” The [Washington Post](#) (1/18, Goldfarb, Mui, 11.43M) reports that Ross “did not elaborate...on what those punitive measures might entail, although Trump has repeatedly called for a border tax on U.S. companies that offshore jobs and sell their products back home.”

The [New York Times](#) (1/18, Rappeport, Huetteman, Subscription Publication, 13.9M) quotes Ross as saying, “As to Canada and Mexico, the President-elect has made no secret in his public remarks, nor have I, that NAFTA is logically the first thing for us to deal with. We ought to solidify

relationships the best way we can in our own territory before we go off into other jurisdictions.”

The [Wall Street Journal](#) (1/18, Leubsdorf, Subscription Publication, 6.37M) reports that Ross also stressed tougher enforcement of existing rules, rather than the imposing of new tariffs. [Politico](#) (1/18, Behsudi, Palmer, 2.46M) also reports on Ross’ remarks.

Price Vows To Protect Access To Health Coverage, Denies Investment Wrongdoing.

Coverage of HHS Secretary-designate Tom Price’s appearance before the Senate Health, Education, Labor, and Pensions Committee is divided between questions surrounding Price’s stock trading and Price’s comments on the plan to replace the Affordable Care Act.

On [ABC World News Tonight](#) (1/18, story 2, 4:45, Muir, 14.63M), Mary Bruce reported that Price was asked if he has seen the plan President-elect Trump says he has to replace the ACA, as well as “on the President-elect’s promise earlier this week that his plan would include ‘insurance for everybody.’ The Congressman wouldn’t go that far.” Price: “I look forward to working with you to make certain that every single American has access to the highest quality care and coverage that is possible.” Price was also “grilled on ethics, questions about whether he bought stock in healthcare companies as he was writing legislation to help them.” Sen. Elizabeth Warren asked “what happened when Price found out about the stock purchase” by his broker. Warren: “Did you take an additional actions after that date to advance your plan to help the company that you now own stock in?” Price: “I’m offended by the insinuation, Senator.”

On [NBC Nightly News](#) (1/18, story 2, 2:30, Holt, 16.61M), Tom Costello said Price is “controversial with Democrats because he’s been working to repeal Obamacare, and because they say he’s been buying and selling stocks in medical companies that they claim he’s also tried to help or could have tried to help through legislation. On Capitol Hill today, fireworks over Obamacare and the HHS nominee’s refusal to promise he won’t touch Medicaid or Medicare.” Warren: “You might want to print out President-elect Trump’s statement, ‘I am not going to cut Medicare or Medicaid.’ and post that above your desk in your new office.” Costello: “Price offered few specifics but insisted he wants more access to affordable health insurance with more choices.” On the [CBS Evening News](#) (1/18, story 6, 2:15, Pelley, 11.17M), Nancy Cordes reported Democrats “were coming down hard” on Price, who “would implement the GOP’s currently uninformed replacement for Obamacare.”

[USA Today](#) (1/18, O’Donnell, 5.28M) reports Price told the panel that “nobody, including those with mental health and addiction disorders, should lose access to health insurance,” a position that “is at odds with Republican plans

to replace the existing law with bills that would curtail the expansion of Medicaid and eliminate tax credits to buy insurance.” That statement “also highlights the changing nature with which Obamacare replacements are being discussed” by Trump “and his key nominees, such as Price.”

The [New York Times](#) (1/18, Pear, Subscription Publication, 13.9M) reports that Price “promised on Wednesday to ‘make sure that nobody falls through the cracks’ if the ACA is repealed. He “set lofty goals for a health law that would replace President Obama’s signature domestic achievement, but he did not say how he would achieve those goals.” Price also “denied any impropriety in his trading of stocks in health care and pharmaceutical companies, saying he left many details to his broker.” The [Washington Times](#) (1/18, Howell, 272K) says Democrats “said his health policies would erode care and be devastating for Americans.”

The [Washington Post](#) (1/18, A1, Eilperin, Goldstein, 11.43M) says Democrats “pressed hard on whether he used insider knowledge to enrich himself or pushed bills benefiting companies in which he had a financial stake,” but Price “maintained that he had not sought to take advantage of his public position and that he was not aware of what precise stocks he held in the past or at present.”

The [New York Post](#) (1/18, Schultz, 3.82M) reports under the headline “Tom Price Forced To Go On Defensive At Senate Hearing” that Price “batted down allegations Wednesday that he might have broken the law on his stock investments.” [Politico](#) (1/18, Diamond, 2.46M) says Democrats “hammered” Price on the subject, but he “survived a contentious hearing Wednesday that seemed designed to slow, if not stall, his confirmation to a role in which he will help dismantle the Affordable Care Act.” [McClatchy](#) (1/18, Clark, 74K) also has a report.

The [Washington Post](#) (1/18, 11.43M) says in a critical editorial that on ACA replacement, “Price offered some big promises – but scant reassurance,” while on the stock question, Price’s “general defense – that his broker was responsible for trading his portfolio and that he followed House ethics rules – did not settle these questions.” Dana Milbank writes in his [Washington Post](#) (1/18, 11.43M) column that Price “has found a miracle cure for ailing investment portfolios.” Milbank writes, “Each day of the Trump transition seems to deliver a new blow to the embattled notion of honest government. ... It all feels a bit, well, swampy.” But the [Wall Street Journal](#) (1/18, Subscription Publication, 6.37M) says in an editorial that the Price stock issue shows that nonprofessional investors should opt for index funds over individual securities, and that this would be particularly wise for political figures wary of the appearance of conflicts of interest.

The [Washington Post](#) (1/18, A1, Tumulty, Wagner, O’Keefe, 11.43M) reports on its front page that Price was just

one of three Trump Cabinet picks who “came under growing fire Wednesday on ethical issues, potentially jeopardizing their nominations.” Office of Management and Budget Director-designate Mick Mulvaney and Commerce Secretary-designate Wilbur Ross both face questions over household employees.

Mulvaney Failed To Pay Employment Taxes For Household Worker.

The [Washington Post](#) (1/18, Snell, 11.43M) reports that Office of Management and Budget Director-designate Mick Mulvaney, “failed to pay more than \$15,000 in state and federal employment taxes for a household employee,” according to a disclosure form obtained by the Post. While Mulvaney told the Senate Budget Committee that he “paid \$15,583.60 in back taxes to the federal government but similar oversights brought down the nominations of several past nominees.”

The [New York Times](#) (1/18, Steinhauer, Subscription Publication, 13.9M) reports that a spokesman for Budget Chairman Mike Enzi said he “would have no immediate comment. Mr. Mulvaney will almost certainly be asked about the issue at his hearing, and Republicans on the committee are most likely aware of its existence.” The [Washington Times](#) (1/18, Sherfinski, 272K) reports that President-elect Trump’s “team rallied behind the South Carolina congressman,” saying in a statement, “Nobody is more qualified and more prepared to rein in Washington spending and fight for taxpayers than Mick Mulvaney.”

Media Analyses: Pruitt Takes Aggressive Stance During Confirmation Hearing.

The [New York Times](#) (1/18, Davenport, Subscription Publication, 13.9M) reports that EPA Administrator-designate Scott Pruitt “went on the offensive in his Senate confirmation hearing on Wednesday, criticizing federal rules protecting air and water and addressing climate change, and forcefully advocating a states’ rights approach to environmental regulation.” Senate Environment and Public Works Committee Democrats “aggressively pressed” Pruitt on his record as Oklahoma attorney general, “noting that he has sued the E.P.A. 14 times in an effort to block federal air and water pollution regulations.” The [Washington Post](#) (1/18, Dennis, 11.43M) reports that Pruitt “declined to say Wednesday whether he would recuse himself from those ongoing cases if confirmed as the agency’s new leader.”

The [Washington Times](#) (1/18, Wolfgang, 272K) says Pruitt “has been a leading thorn in the side of the EPA for the last six years.” He told the committee that “the country wants change at the EPA and that he’s committed to both protect the environment and take advantage of the nation’s vast energy resources.”

The [Washington Post](#) (1/18, Weigel, 11.43M) additionally reports that while Democrats “tried to grill Pruitt over donations” from energy firms “that he would be in charge of regulating,” Republicans “turned that line of questioning against the Democrats, saying they were trying to undermine a good man – and the good people of a major American industry.”

NYTimes Analysis: Perry “Initially Misunderstood” Role Of Energy Secretary. The [New York Times](#) (1/18, Davenport, Sanger, Subscription Publication, 13.9M) writes somewhat critically about Energy Secretary-designate Rick Perry’s “learning curve” as he “pursues a job he initially misunderstood.” While Perry believed he would become “a global ambassador for the American oil and gas industry that he had long championed” in Texas, he discovered that as DOE chief, “he would become the steward of a vast national security complex he knew almost nothing about,” caring for the US nuclear arsenal. Perry, “who once called for the elimination of the Energy Department,” will go before the Senate Energy Committee today.

Media Analyses: DeVos Faced “Bumpy” Hearing, Appeared Unprepared. Analysis and commentary regarding Education Secretary-designate Betsy DeVos’ Tuesday evening confirmation hearing is harshly negative. [Politico](#) (1/18, Hefling, Emma, Wermund, 2.46M) reports that DeVos “has gone viral – and not in a good way. After her bumpy confirmation hearing Tuesday night,” DeVos “was a social media sensation Wednesday,” with online video clips showing DeVos “struggling to answer questions about the best way to measure student performance.” And while “her suggestion that allowing states to permit guns in and around schools could help protect against grizzly bears was relentlessly mocked on Twitter,” perhaps the “most damaging was DeVos’ suggestion that states should handle enforcement of a federal law that protects the civil rights of children with disabilities.” On [NBC Nightly News](#) (1/18, story 3, 1:35, Jackson, 16.61M), Hallie Jackson reported that the “typically tame hearing for education secretary turned fiery” Tuesday evening for DeVos. NBC ran clips of critical questions and comments from Sens. Al Franken, Chris Murphy, and Bernie Sanders.

The [New York Times](#) (1/18, Subscription Publication, 13.9M) says in an editorial that DeVos “refused multiple times to agree that traditional public and charter schools should be held to the same level of accountability,” and “seemed unaware of some of the basic functions of the education department.” DeVos “also won the tin ear award hands down. When Christopher Murphy asked whether she would agree that schools are no place for guns, she did not give the

obvious right answer to a Democratic senator whose state suffered the horrendous Sandy Hook massacre,” suggesting “in a transcendently odd moment...that schools in places like Wyoming might need a gun ‘to protect from potential grizzlies.’”

In his [Detroit Free Press](#) (1/18, 1.01M) column, Brian Dickerson writes that “even a truncated confirmation hearing designed to limit the nominee’s exposure couldn’t conceal the myriad ways” in which DeVos “is unprepared for the responsibility she is about to assume.” Dickerson writes that DeVos “appeared to be unaware” of a federal law protecting disabled students, and “appeared confused by a question seeking her views on the debate between reformers who want schools to enforce a single standard of competency and those who want to incentivize academic growth.”

WPost Analysis: DeVos Could Bring Change To Sexual Assault Policy. The [Washington Post](#) (1/18, Anderson, 11.43M) writes that “through what she said and what she didn’t,” DeVos “indicated during her hearing Tuesday evening the strong possibility of a new approach to federal civil rights enforcement related to sexual violence.” The Education Department’s Office for Civil Rights “was a key player in what has become a six-year campaign to combat sexual assault in schools” under President Obama, but an exchange between DeVos and Sen. Bob Casey over Title IX suggested a possible shift.

McCain Says He Remains “Very Concerned” About Tillerson. [Politico](#) (1/18, Everett, 2.46M) reports that Sen. John McCain told CBS on Wednesday that he is undecided on the nomination of Secretary of State-designate Rex Tillerson. McCain said, “I am very concerned about someone who took a friendship award from Vladimir Putin, who’s a butcher. Actually what Vladimir Putin is, he’s a KGB agent. That’s all.” Politico notes that if McCain and fellow GOP Tillerson critics Sens. Lindsey Graham and Marco Rubio vote against him, his nomination could fail. However, McCain told Fox News earlier this week that he is leaning in Tillerson’s favor.

Former OneWest Mortgage Customers Come To Capitol Hill To Criticize Mnuchin. [Reuters](#) (1/18, Lynch) reports that borrowers who say OneWest Bank, which was once run by Treasury Secretary-designate Steven Mnuchin, “refused to help them when they struggled to pay their mortgages” appeared at a Wednesday Capitol Hill event organized by Senate Democrats. They included “an 86-year-old woman who said the bank ordered her to pay off a reverse mortgage or get out of her house after her husband died.” Another attendee, who lost her home after she was unable to secure a loan modification, said, “Steve Mnuchin’s

company had no interest in helping us. They wanted to foreclose because they were focused on their profits.”

[USA Today](#) (1/18, McCoy, 5.28M) reports that a Mnuchin representative did not respond to a request for comment, nor did CIT Bank, which now includes OneWest. However, [Bloomberg News](#) (1/18, Dexheimer, Mohsin, 2.41M) reports that in prepared remarks for his confirmation hearing today, Mnuchin says, “Since I was first nominated to serve as Treasury secretary, I have been maligned as taking advantage of others’ hardships in order to earn a buck. Nothing could be further from the truth.”

Mnuchin’s IndyMac Acquisition Defended. In a [Wall Street Journal](#) (1/18, Subscription Publication, 6.37M) op-ed, John Bovenzi and Jim Wigand, who were both involved in Mnuchin’s 2009 acquisition of the failed IndyMac, write that the acquisition was aboveboard and that criticism of Mnuchin is political in nature.

Trump To Nominate Perdue For USDA. [Reuters](#) (1/18) reports that President-elect Trump will nominate ex-Georgia Gov. Sonny Perdue to be agriculture secretary today, according to a senior transition official. The [Atlanta Journal-Constitution](#) (1/18, Bluestein, 1.41M) says Trump “went down to the wire with the Perdue pick, making him his last Cabinet selection before he is sworn into office Friday. The choice was mired in political wrangling, with some factions pushing Trump to opt for someone from the Midwest or to diversify his Cabinet by naming a Hispanic official.”

The [New York Times](#) (1/18, Davis, Haberman, Subscription Publication, 13.9M) reports that Perdue “was a loyal supporter of Mr. Trump during his campaign.” [Politico](#) (1/18, Boudreau, Dawsey, Isenstadt, 2.46M) says the pick is “likely to please farm groups while angering those who have called for more diversity” in the Cabinet.

Todd Gillman writes in the [Dallas Morning News](#) (1/18, 1.12M) that the Perdue pick means that Trump’s Cabinet “is poised to become the first since 1988 without any Hispanic officials. ... Two Hispanic Texans were under consideration for the post: former U.S. Rep. Henry Bonilla, a San Antonio Republican, and Elsa Murano, a former Texas A&M president and former undersecretary for food safety.”

Army Secretary Nominee Was Accused Of Punching Concessions Worker Last Summer.

The [New York Times](#) (1/18, Schmidt, Subscription Publication, 13.9M) reports that Vincent Viola, “the billionaire Wall Street trader” nominated by President-elect Trump to be secretary of the Army, “was accused in August of punching a concessions worker at a high-end racehorse auction” in Saratoga Springs, New York. While police officers did not witness the episode, when officers arrived at the scene, “the concessions worker had a ‘swollen bloody lip’ and said that

Mr. Viola had punched him in the face, according to the police report.”

Commodity Futures Trading Commission Enforcement Chief Stepping Down.

The [New York Times](#) (1/18, Protes, Subscription Publication, 13.9M) reports, “One of the Obama administration’s few remaining Wall Street enforcers is stepping down.” Aitan Goelman, who is in charge of enforcement at the Commodity Futures Trading Commission, announced Wednesday that he will depart as of February 3 – part of “a broad exodus of prosecutors and regulators in the Obama administration’s final days.”

Trump Has Not Selected Official White House Photographer.

The [New York Post](#) (1/18, Tacopino, 3.82M) reports in a brief item that President-elect Trump “has reportedly not named an official White House photographer, bucking a tradition that started with President Lyndon Johnson.”

Christie Says He Turned Down Several Posts Because Of Wife’s Objections.

The [New York Post](#) (1/18, Fredericks, 3.82M) reports that Gov. Chris Christie said in a Wednesday radio interview that “he turned down several Trump administration jobs because wife Mary Pat told him if he moved to Washington.” Christie said, “[Trump] didn’t offer me a job that I thought was exciting enough for me to leave the governorship. Because Mary Pat made really clear she wasn’t coming to D.C.”

Ways And Means Chairman Defends “Border-Adjustable Tax Provision.”

[Reuters](#) (1/18, Morgan) reports House Ways And Means Committee Chairman Rep. Kevin Brady on Wednesday “defended his border-adjustable tax provision against criticism from President-elect Donald Trump.” In interview on CNBC, Brady said, “I’m absolutely confident that we can move this provision forward.” The measure has been opposed by “import-dependent industries” and Trump has called it “too complicated.” Then on Wednesday, in an interview at Axios, Trump said it was still being considered.

USA Today Analysis: Recent Job Announcements Partly Effort To Gain Favor With Trump.

[USA Today](#) (1/17, Woodyard, 5.28M) reports that announcements by companies of employees being added in the US are growing from a “trickle” to a “cascade” in an effort to gain “favor with President-elect Donald Trump.” Still, USA Today questions whether these companies “are actually changing direction away from expanding in other countries,” and cites economists saying its

a combination of real change and announcing decisions they had already made. USA Today also says the announcements “sound great,” but the numbers of jobs “pale in comparison to the jobs lost over the years.” As an example it points out that in 1979 GM’s US workforce was “above 618,000” but is now about 56,000.

Chicago Police Officer Charged With First-Degree Murder In Off-Duty Shooting. The [Chicago Tribune](#) (1/18, Hinkel, 2.54M) reports that a veteran Chicago police officer has been arrested on charges of first-degree murder “in the off-duty shooting of a 38-year-old man on the Northwest Side earlier this month.” Cook County prosecutors on Wednesday filed charges against Lowell Houser in the January 2 shooting death of Jose Nieves, according to Tandra Simonton, a spokeswoman for the state’s attorney’s office. Authorities “have given little detail on the shooting, but police have said that Nieves was not armed and that he and the officer had argued in the past.” Houser, 57, a 28-year department veteran, “is in custody and expected to appear in bond court Thursday, Simonton said.” The Tribune notes that “charges against local police officers in shootings, on- or off-duty, are rare, but Houser marks the second Chicago police officer to face a serious criminal charge within days.”

Obama Administration Races To Finish Corporate Probes. The [Wall Street Journal](#) (1/18, A1, Viswanatha, Subscription Publication, 6.37M) reports on its front page that the Obama Administration is pressing to completion a series of big business probes before President-elect Trump’s inauguration, reaching settlements worth approximately \$20 billion in the past week with banks, automobile makers, drug companies, and other firms. The settlements involve allegations of financial misdeeds, emissions cheating, lending discrimination, and antitrust violations. Observers told the Journal that such last-minute flurries of prosecutorial activity are common in the waning days of presidential administrations, but that the volume of the recent settlements is unusually high.

Labor Department Sues Oracle, Claiming It Pays White Men More Than Others. The [AP](#) (1/18) reports that the Department of Labor has filed a lawsuit against Oracle, “claiming that the technology giant has a ‘systemic practice’ of paying white male workers more than their non-white and female counterparts with the same job titles.” The lawsuit also alleges that the company “favors Asian workers in its recruiting and hiring practices for product development and other technical roles, which resulted in hiring discrimination against non-Asian applicants.” In a statement, Oracle Corp. on Wednesday “called the lawsuit ‘politically motivated, based on false allegations and wholly

without merit.” The Labor Department said the lawsuit “is the result of a review of Oracle’s equal employment opportunity practices at its headquarters in Redwood Shores, California,” and according to the suit, Oracle “has refused to comply with the agency’s ‘routine requests’ for employment data and records.”

JPMorgan Chase Settles Investigation Over Discriminatory Lending. The [New York Times](#) (1/18, Corkery, Subscription Publication, 13.9M) reports on a settlement with JPMorgan Chase in which it will “pay \$55 million to settle an investigation into whether it charged thousands of African-American and Hispanic borrowers higher interest rates on mortgages than white customers.” JPMorgan issued a statement saying the settlement concerned “legacy allegations that relate to pricing set by independent brokers.”

CFPB Lawsuit Says Navient Cheated Borrowers. [USA Today](#) (1/18, McCoy, 5.28M) reports that the CFPB sued Navient, the nation’s largest student loan servicer on Wednesday “over allegations that it has ‘systematically and illegally’ failed borrowers.” According to the federal lawsuit filed in the middle district of Pennsylvania, Navient “created repayment obstacles for tens of thousands of student borrowers by providing incorrect payment information, processing payments incorrectly and failing to act when borrowers complained.” In addition, the suit accuses the company of “cheat[ing] borrowers out of their rights to lower repayments,” and “seeks financial relief for student borrowers who were harmed.”

ED Drops “Supplement Not Supplant” Rule Under “Every Student Succeeds” Act. [Politico](#) (1/18, Emma, 2.46M) reports the US Department of Education withdrew its proposed “supplement not supplant” regulation under the Every Student Succeeds Act. The decision is “a blow to civil rights groups” and “a win” for Senate Education Committee Chairman Lamar Alexander (R-TN) and Republican lawmakers who “threatened to kill the rule if the department moved forward.”

Media Analyses Ponder Obama’s Legacy. A [New York Times](#) (1/18, Schuessler, Subscription Publication, 13.9M) analysis focuses on Obama’s “legacy as a historian,” reporting that “some scholars see in him a man who used the presidency not just as a bully pulpit but also as something of a historian’s lectern.” Obama has “positioned his own rise as a step toward fulfillment of America’s ideals of liberty and equality, while also drawing a straight line through ‘Seneca Falls and Selma and Stonewall,’ as he put it in his second Inaugural.”

Greg Ip writes in the [Wall Street Journal](#) (1/18, Ip, Subscription Publication, 6.37M) that Obama found that the country's taste for change was not as strong as his own, and while he was successful at implementing some economic reforms, other efforts, any of which he undertook via executive order, are vulnerable to the incoming Trump Administration, Congress, and the courts.

On [NBC Nightly News](#) (1/18, story 11, 2:00, Holt, 16.61M), correspondent Harry Smith highlighted how the President has changed over his eight years in office, reporting that "the job does something to you. There is a weight, there's a responsibility that can't be measured. Look at other presidents. Their faces are like an odometer of human experience. Over the years, you see them rack up the miles."

Obamas To Vacation In Palm Spring Following Trump's Inauguration. [ABC World News Tonight](#) (1/18, story 10, 1:10, Davis, 14.63M) reported that following Friday's inauguration ceremony, the Obama family will be flown "to Joint Base Andrews where they'll take one final flight aboard the presidential plane, no longer called Air Force One, which is also reserved for the current President, en route to Palm Springs for vacation."

Trump Insiders Expect "Wild First Week," "Shock And Awe Strategy" With Executive Actions. In his "Talking Points Memo" segment on [Fox News' The O'Reilly Factor](#) (1/18, 767K), Bill O'Reilly said there is "word from inside the Trump organization that the new President will institute a 'shock and awe strategy' and sign a number of far-reaching executive actions to signal that he will shake up Washington." If that occurs, "all hell will break loose." O'Reilly concluded saying, "Americans can expect a wild first week Donald Trump was President. He will issue a number of executive orders, Democrats will not be happy with them, and the media condemnation will be intense."

Trump Could Reverse Obama Orders Benefiting Contract Workers. In his "Federal Insider" column for the [Washington Post](#) (1/18, 11.43M), Joe Davidson writes that when President-elect Trump takes office, he could wipe out executive actions, memoranda, and orders issued by President Obama "to improve the lot of individual federal contract workers and shape the balance between contractors and government employees." According to an August 2015 letter from four government contracting associations – the Aerospace Industries Association, National Defense Industrial Association, Professional Services Council and Information Technology Industry Council – to White House Chief of Staff Denis McDonough and Senior Adviser Valerie Jarrett, Obama "had issued 12 government contracting executive orders

resulting in 16 new regulations." The associations' letter argued that "the impacts, inefficiencies, and in many cases, unintended consequences" of the regulations "are such that the interests of the American taxpayer are being significantly and negatively impacted."

Bush 41, Wife Hospitalized In Texas. [USA Today](#) (1/18, Jackson, 5.28M) reports that former president George H.W. Bush has been hospitalized in an intensive care unit for "an acute respiratory problem stemming from pneumonia," according to family spokesman Jim McGrath, who said former first lady Barbara Bush is also in Houston Methodist Hospital "as a precaution after experiencing fatigue and coughing." McGrath said of the former president, "Doctors performed a procedure to protect and clear his airway that required sedation. ... President Bush is stable and resting comfortably in the ICU, where he will remain for observation." Phillip Mena reported in the lead story on [ABC World News Tonight](#) (1/18, lead story, 2:20, Muir, 14.63M) that doctors "are happy about how that procedure went" and are now "in a wait and see mode." The [New York Times](#) (1/18, Baker, Subscription Publication, 13.9M) says that following "initial reports of Mr. Bush's hospitalization, his office said he was expected to return home by the weekend."

In the lead story for [NBC Nightly News](#) (1/18, lead story, 2:25, Holt, 16.61M), correspondent Gabe Gutierrez said that "well wishes are pouring in from around the world." The [CBS Evening News](#) (1/18, story 8, 1:30, Pelley, 11.17M) reported that President Obama "offered the Bushes his best wishes at his final press conference." Obama: "They have been a constant source of friendship and support and good counsel for Michelle and me over the years. They are as fine a couple as we know." President-elect Trump also expressed hope that the Bushes will recover soon, writing in a [tweet](#) Wednesday evening, "Looking forward to a speedy recovery for George and Barbara Bush, both hospitalized. Thank you for your wonderful letter!"

Trump A Target At DNC Candidates Forum. Seven candidates vying to become the next DNC chair on Wednesday took part in a forum at George Washington University hosted by the Huffington Post. Unsurprisingly, President-elect Trump was a focus of the forum. Under the headline "DNC Candidates Sound The Alarm On Trump," [Politico](#) (1/18, Strauss, 2.46M) reported that Labor Secretary Tom Perez said at the beginning of the event, "Donald is our president in 48 hours or less. We need a leader in the party who's a leader, who's a fighter, who's a proven progressive, who can be a communicator, who can be a turnaround specialist." Asked whether "Democrats should try and work with Trump or resist him, the universal response was resist." For example, Rep. Keith Ellison (D-MN) is quoted as saying Trump "has already shown us where he stands. From the

very beginning, he put in Steve Bannon, who is a renowned white supremacist and misogynist and then he proceeded to put someone in [the Labor Department] who is an anti-labor candidate.”

The [Washington Post](#) (1/18, Weigel, 11.43M) reports that during the forum, Ellison “said for the first time that he will ask Sen. Bernie Sanders (I-Vt.) to share the donor list built during his 2016 presidential campaign, answering a question that had begun to unsettle the” DNC contest. The Post says the candidates have “resisted the early framing of the race as a re-fight of the 2016 primary; the fate of Sanders’s email list had become part of that story, with” Sanders saying “last week that he would ‘cross that bridge’ once the DNC race was settled.” Sanders has endorsed Ellison’s bid.

On its website, [CNN](#) (1/18, Bradner, 29.79M) reported that Ellison said “he’d push the reluctant Sanders to hand his massive list of supporters over to the DNC. ‘We’re going to call upon everybody to give all the resources they have,’” asserted Ellison, who “said Democrats are ‘in an emergency’ as they face the beginning of...Trump’s presidency. ‘Everybody has to give up what they have to maximize turnout and agency and organization,’ he said.”

The [Minneapolis Star Tribune](#) (1/18, Sherry, 1.27M) reports that the candidates “split on how to respond to...Trump, with some saying state parties need to be more involved. Others – including Ellison and Perez – said Democrats need to take the high road and promote messages of how the party is going to fight for regular working-class people. ‘He is what we call a target-rich environment,’ Perez said of Trump. ‘You can’t meet him tweet for tweet. We really gotta understand you don’t go to a knife fight with a spoon.’”

However, [The Hill](#) (1/18, Kamisar, Easley, 1.25M) said the candidates “offered little disagreement over how to rebuild the party...coalescing around the need to hold...Trump’s feet to the fire over the next four years.” The Hill added that “there was widespread agreement about the path forward – a return to a 50-state strategy, a messaging improvement, a retooled primary process and opposition to Trump – along with praise for the other candidates on stage.” The [Washington Times](#) (1/18, McLaughlin, 272K) reports that the candidates “universally agreed via a show of hands that the party should be more involved in organizing protests with Mr. Trump in The White House.”

Quinnipiac Poll: Clinton Would Beat De Blasio In NYC Mayoral Race. The [New York Times](#) (1/18, Goodman, Subscription Publication, 13.9M) reports that a new Quinnipiac University [poll](#) found that “a plurality of New Yorkers” say Mayor Bill de Blasio “does not deserve re-election, but no challenger could beat him” with the exception of Hillary Clinton. According to the poll, the first conducted

since rumors of a possible Clinton mayor bid surfaced, if Clinton were to run as an independent, she “would beat Mr. de Blasio in a head-to-head race, 49 to 30 percent.” The Times says that while the result “is not a surprise considering that Mrs. Clinton beat President-elect Donald J. Trump easily in New York City in November,” it “would be a surprise if she decided to announce a run.”

NASA, NOAA Say 2016 Was Hottest Year On Record.

The [Los Angeles Times](#) (1/18, Khan, 4.52M) reports that independent analyses by NASA and NOAA show that 2016 “was the hottest year on record in more than 100 years of record-keeping.” According to NOAA, this is “the third year in a row that global temperatures have reached record-shattering levels,” and NASA “added that the global average temperature for 2016 was 1.78 degrees higher than a baseline period between 1951 and 1980.” According to [USA Today](#) (1/18, Rice, 5.28M), “data sets in the United Kingdom and Japan this week also concurred with the findings from the U.S. agencies.” The [Washington Post](#) (1/18, A1, Mooney, 11.43M) calls the analyses “a powerful testament to the warming of the planet,” and says that the record “comes just two days before Donald Trump, who has tweeted that global warming is a ‘hoax,’ assumes the presidency.” [NBC Nightly News](#) (1/18, story 5, 0:25, Holt, 16.61M) also reported on the NASA and NOAA findings.

Group Plans \$10 Million Campaign On Behalf Of Trump’s Supreme Court Nominee.

The [Washington Times](#) (1/18, Boyer, 272K) reports that the Judicial Crisis Network plans “a \$10 million campaign” to fight for President-elect Trump’s Supreme Court nominee. The conservative network will “pressure campaign against vulnerable Senate Democrats who are up for re-election next year” with a campaign that “will include paid advertising, grass-roots pressure and other activities.”

Pence Likens Trump To Reagan.

In an interview with [USA Today](#) (1/18, Groppe, 5.28M), Vice President-elect Pence likened President-elect Trump to President Ronald Reagan, describing him as a “transformational leader” who will be able to overcome divisions within the GOP and Democratic opposition to get things done. Pence, who “made comparisons between Reagan and Trump throughout the campaign,” said that Reagan provided “that kind of broad shouldered leadership that said on that January day in 1981 that he’d come to Washington, DC, to change it.” He added, “A generation later, we’ve come to a very similar time, with a very similar leader. ... It just informs me that that last administration that revived the country and literally changed the world, is a good place for me to look for an example of a vice president who supports a president like that.”

WPost Analysis: Trump Modeling His Governing Style After Theodore Roosevelt. A [Washington Post](#) (1/18, Rucker, 11.43M) analysis says President-elect Trump “continue to hector businesses” with “almost daily” Twitter posts and in private meetings as he tries to “put the bully back into the bully pulpit, modeling his governing style after Theodore Roosevelt, the president whose attacks on industry barons inspired the term.” Trump is seeking “to change the behavior of corporations – not to mention the intelligence community and other creatures of Washington – through force of intimidation.” He is “a modern-day Roosevelt, who from the White House in the 1900s demonized banks, railroads and other businesses he viewed as insufficiently nationalist.” However, while the “list of major companies announcing U.S. jobs in recent weeks has ranged from Hyundai Motor Co. to Amazon, and in each case Trump and his aides have trumpeted their announcements and claimed credit,” it is not clear “how much the president-elect’s threats influenced their actual business plans.”

Pence Praises Obama Administration’s Handling Of Transition. Vice President-elect Pence told [Fox News’ Special Report](#) (1/18, 1.53M) that the transition has been “orderly, cordial, professional. The President-elect and I have been externally grateful for the cooperation of President Obama, Vice President Biden, and all of their team. It’s put us in a position to be ready on day one to go to work for the American people.”

Distrust Between Trump Transition, Obama Appointees Slows Handover Of Agency Responsibilities. [Politico](#) (1/18, Dawsey, Restuccia, 2.46M) reported that a “deep distrust has taken hold between [President-elect] Trump’s transition officials and Obama’s political appointees at a number of federal agencies, slowing down the handover of agency responsibilities.” Trump “gives conflicting signals and is often in disagreement with his Cabinet nominees,” which has resulted in “confusion over policy on several major agenda items.” Moreover, “people close to the transition” say that “a number of federal agencies are far from having the staff they need to run on Day One.” Politico added that while “a feeling of disarray” is no uncommon during a transition, “some observers — both those loyal to Obama and Trump and others who are more neutral — say this transition is more drama-filled and uneven across federal agencies than some of its predecessors” and that “disorder could have a real impact on Trump’s ability to quickly deliver on his ambitious agenda in the opening weeks of his administration.”

Trump Delivers “Free Flowing” Speech At Dinner Honoring Pence. The [New York Times](#) (1/18, Haberman, Subscription Publication, 13.9M) reports that during a dinner honoring Vice President-elect Pence

Wednesday evening, President-elect Trump delivered “a free-flowing speech” during which he “jabbed at his new Republican allies and his critics alike, questioned the ethics of ‘super PACs,’ and talked about creating a ‘merit-based’ immigration system.” Trump “lauded...Pence in a roughly 25-minute speech, but poked at him for declining to endorse his candidacy in the primary in Indiana, where he was governor, instead backing Senator Ted Cruz of Texas.” Trump “also took aim at Mr. Cruz,” Wisconsin Gov. Scott Walker, members of the “Never Trump” movement, and casino magnate Sheldon Adelson.

Trump Won’t Move White House Press Briefing Room, But Will Choose Who Gets In. [U.S. News & World Report](#) (1/18, Levy, 1.02M) reported that in an interview on “Fox and Friends” Wednesday, President-elect Trump “backed away” from incoming White House chief of staff Reince Priebus’ suggestion that the White House press briefing room might be moved to a larger space in the Eisenhower Executive Office Building, next door to the White House. Trump told Fox News that “his administration won’t move the press out of the White House after all,” but “limited seating in the James S. Brady Press Briefing Room means his team will have to pick and choose who has access to the West Wing space.” Trump said, “The press went crazy, so I said, ‘Let’s not move it.’ ... But some people in the press will not be able to get in.”

Yellen: Fed Will Not Be Deterred By “Short-Term Political Pressures.” In a speech to the Commonwealth Club in San Francisco on Wednesday, Fed Chairwoman Yellen did not mention President-elect Trump or his policy proposals and instead defended the Fed’s mission of promoting a strong economy unencumbered by what she described as “short-term political pressures,” the [Wall Street Journal](#) (1/18, Harrison, Subscription Publication, 6.37M) reports. Yellen said that as of last month most Fed officials, including herself, anticipate raising short-term interest rates several times a year through 2019.

[Bloomberg News](#) (1/18, Torres, 2.41M) says Yellen told her audience that the economy is “close” to the Fed’s goals of full employment and stable prices and she expressed confidence that improvements will continue. Yellen said, “It is fair to say the economy is near maximum employment and inflation is moving toward our goal,” and added that while “it makes sense to gradually reduce the level of monetary policy support,” the timing of the next interest-rate increase “will depend on how the economy actually evolves over coming months.”

Stocks Gain After Yellen Speech. [Reuters](#) (1/18, Carew) reports that stocks “gained ground” Wednesday in the wake of Yellen’s indication that the Fed “was ready to raise

interest rates quickly this year.” While the Dow lost 22.05 points to close at 19,804.72, the S&P 500 added 4 points to finish at 2,271.89, and the Nasdaq ended the day 16.93 points higher at 5,555.65.

Fed Reports Modest Growth In Most Of Country. [USA Today](#) (1/18, Davidson, 5.28M) reports that the Federal Reserve said Wednesday that the economy “expanded modestly in most of the country late last year, with manufacturing rebounding and retail sales increasing, but the holiday shopping season was generally disappointing.” According to the Fed’s “beige book,” which covered late November through December, “manufacturers in most regions ‘reported increased sales with several citing a turnaround versus earlier in 2016.’” While job growth “grew at a ‘slight to moderate’ pace as wages rose modestly,” many regions “continued to struggle to find skilled workers in the tightening labor market, and several even faced hurdles ‘recruiting for less skilled jobs.’”

Experts Say Trump’s Plan For Business Assets Leaves Unanswered Questions. The [Wall Street Journal](#) (1/18, Berzon, Subscription Publication, 6.37M) reports that legal and business experts say the details of President-elect Trump’s plan to separate his presidency from his business assets. These experts say the plan Trump announced last week leaves many questions unanswered including what, if any, restrictions would be placed on lobbying by Trump’s sons, who will run the business, or other company executives, whether the company will accept foreign money for US-based projects, and how the trust will be enforced, among others.

The [New York Times](#) (1/18, Yourish, Andrews, Subscription Publication, 13.9M) reports that the Trump Organization and its marketing partners have been removing Trump and his daughter, Ivanka, from their websites over the last week and have stepped up those efforts in the last two days. While Federal ethics rules which “prohibit government employees from using their images to sell products,” do not apply to the president, “previous White House ethics offices have acted as if they do.” The Times goes on to cite a number of examples of the changes being made by the Trump Organization and its partners. In a separate story, the [New York Times](#) (1/18, Haberman, Lipton, Subscription Publication, 13.9M) cites a statement from Trump Organization spokeswoman Amanda Miller, who said, the company will “no longer actively utilize Donald Trump’s image or likeness for the marketing or promotion of the Trump Organization and its portfolio of properties. ... This applies to both owned and licensed properties in both the United States and abroad.” According to the company, the process “will take some time to resolve, given how frequently his name is used.”

Fowler Laments Lack Of Online Tools To Hold Politicians Accountable. In a piece for the [Wall Street Journal](#) (1/18, Fowler, Subscription Publication, 6.37M), personal technology columnist Geoffrey Fowler writes that consumer-friendly online tools to enable citizens to hold politicians accountable are lacking. Fowler’s column provides an overview of the nonpartisan tools that are available, but he adds that civic technologists have expressed frustration over the amount of work left to do on this front.

Trump Pays \$25 Million To Settle Trump University Suit. [Politico](#) (1/18, Gerstein, 2.46M) reported that President-elect Trump has paid out \$25 million “to settle litigation over his defunct Trump University real estate seminar program.” According to “two sources involved,” Trump University, which is now known as the Trump Entrepreneur Initiative, “transferred the funds Tuesday night.” The funds “will be put into escrow until a judge makes a decision on whether to approve the settlement.” A hearing is set for March 31.

65 House Democrats Say They’ll Boycott Trump’s Inauguration. In a partially updated blog post from the previous day, the [Washington Post](#) (1/18, Viebeck, 11.43M) reported, “There are now more than 60 House Democrats – 65, at last count – who have declared that they will not attend the inauguration” of President-elect Trump on Friday. Repeating from its earlier blog entry, the Post said these lawmakers say they won’t attend Trump’s inauguration in order “to protest what they described as his alarming and divisive policies, foreign interference in his election and his criticism of civil rights icon John Lewis.”

On [ABC World News Tonight](#) (1/18, story 4, 3:15, Muir, 14.63M), David Muir referenced “the boycott” of the inauguration by House Democrats, saying, “It’s 60 and counting. ABC’s Cecilia Vega asking them face to face, is that helping to unify the country?” Vega added, “Democrats I spoke with today defending their decision.” For example, Rep. Lloyd Doggett (D-TX) was shown saying, “If we are to have respect for this President, he has to show respect.” Vega: “But you not going to the inauguration, what kind of respect does that show him?” Doggett: “It says that we question the kind of presidential, unpresidential action which he’s been engaged.” Vega: “Trump’s response?” Trump was shown saying in a Tuesday interview with Fox News: “As far as other people not going, that’s okay, because we need seats so badly, I hope they give me their tickets. Are they going to give us their tickets?”

Democrat Moore To Attend Inauguration, Wants To Be Face Of “The Resistance.” The [Washington Times](#) (1/18, Miller, 272K) reports that Rep. Gwen Moore (D-WI) on Wednesday said that she will attend “the inauguration

because she wanted to stand before...Trump as the face of 'The Resistance.'" In a statement, Moore "said she supports her colleagues decision to" skip the inauguration, "but that she feared Mr. Trump would turn it to his advantage." Moore is quoted as saying, "Knowing how he operates, I suspect President-elect Donald Trump will use this expression of free speech as an excuse to bypass Democrats and to push his extreme agenda with utter impunity. With that in mind, I refuse to be a pawn in the president-elect's efforts to rally support from congressional Republicans. As a proud Democrat, I want President-elect Trump to see me front and center as he's sworn in. I want him to see exactly what his opposition looks like. When he sees me, I want him to see The Resistance."

Rockettes Divided Over Whether Group Should Perform At Trump Inauguration. The [New York Times](#) (1/18, Rogers, Kourlas, Subscription Publication, 13.9M) reports on what it describes as "a rare collision of presidential politics and a venerable arts organization," saying that "current and former Rockettes find themselves in a new kind of spotlight – a position both painful and empowering – as they take sides over" whether to perform at "the inauguration, a split illustrating the cultural divide that...Trump has cleaved through the country."

Ahead Of Women's March On Washington, A "Bitter Rift" Over Abortion. The [New York Times](#) (1/18, Stolberg, Subscription Publication, 13.9M) reports, "Across the country, women who oppose abortion – including one in six women who supported Hillary Clinton, according to a recent survey by the Pew Research Center – are demanding to be officially included in Saturday's Women's March on Washington. But those requests have been spurned, creating a bitter rift among women's organizations, and raising thorny questions about what it means to be a feminist in 2017."

In Op-Ed, Pro-Life Feminist Vows To Take Part In The Women's March. In a [Washington Post](#) (1/18, 11.43M) op-ed, Life Matters Journal founder Aimee Murphy writes that "it is possible to be pro-life and a feminist and opposed to President-elect Donald Trump. It's too bad the organizers of the Women's March on Washington refuse to accept this fact. This week march organizers indicated that women like me are not welcome in their ranks," removing "New Wave Feminists, a pro-life feminist group, as an official partner." Murphy, however, says that those who hold her views "will march. Planned Parenthood does not own women's rights."

Trump Calls Mar-A-Lago His "Winter White House." [Politico](#) (1/18, Caputo, 2.46M) reported that in a [tweet](#) on Wednesday, President-elect Trump dubbed his Mar-a-Lago estate in Palm Beach his "Winter White House." Along

with a picture of him "at the estate penning the first speech he'll give as president of the United States in 48 hours," Trump wrote, "Writing my inaugural address at the Winter White House, Mar-a-Lago, three weeks ago. ... Looking forward to Friday."

Cuomo Tells Trump New York Would Suffer From Cuts In Federal Aid. The [New York Times](#) (1/18, Goodman, Subscription Publication, 13.9M) reports New York Gov. Andrew Cuomo, who met with President-elect Trump on Wednesday, said after the meeting that he had told Trump that New York "benefits from federal support for housing, health care and infrastructure and would be harmed if that support diminished." Cuomo also said the meeting "was not adversarial."

Politico Analysis: Big City Mayors Attack Trump In Hopes Of Boosting Their Profiles. [Politico](#) (1/18, Siders, 2.46M) reports on the US Conference of Mayors at which "big city mayors" took the opportunity to offer "harsh criticism" of President-elect Trump, with Los Angeles Mayor Eric Garcetti offering Los Angeles schools as "places of refuge" for "undocumented immigrants," while Philadelphia Mayor Jim Kenney "mocked the president-elect and his cabinet choices," and New York City Mayor Bill de Blasio has planned a protests at the Trump International Hotel and Tower in Manhattan. Politico says that apart from "a deep aversion to his agenda," the mayors see an "unparalleled political opportunity" to improve "standing with local constituencies" as well as "statewide prospects in blue states." De Blasio, particularly, "has turned to anti-Trump sentiment as a centerpiece of his re-election campaign."

After Murder Of DNC Aide Rich, Conspiracy Theories Ran Amok. The [Washington Post](#) (1/18, Roig-Franzia, 11.43M) runs a piece focusing on Seth Rich, the 27-year old DNC aide who was shot to death in Washington, DC last year, saying, "He was a meme in the weirdest presidential election of our times." The Post says Rich's father, Joel, "wanted to move on to the next stage of grief, but" because of this "era of reckless information," there was too much noise, with "the allegations getting more and more far-fetched. Seth was ordered killed by Hillary Clinton because he knew something about her email scandal. Seth was killed by Russians posing as FBI agents investigating the Clintons. Seth was killed because he slipped DNC emails to WikiLeaks." The Post adds, "What seems painfully obvious to his family is that Seth Rich was, instead, the victim of a botched holdup, one of a series of armed robberies in the neighborhood around that time."

Research Casts Doubt On Influence Of Fake News On Election Result.

The [New York Times](#) (1/18, Irwin, Subscription Publication, 13.9M) reports in its "The Upshot" column that new research by economists Hunt Allcott of New York University and Matthew Gentzkow of Stanford "throws at least a bit of cold water on the theory that false news was a major influence on the election result." Allcott and Gentzkow asked people "whether they had heard various pieces of news that reflected positively or negatively on one of the candidates — of three varieties:" — true news, fake news, "as identified by fact-checking sites like Snopes and PolitiFact," and "fake fake news" they invented. They found that "as many people recalled seeing and believing fake news that had been published and distributed through social media as recalled seeing fake news that had never existed and was purely an invention of researchers," which is "a strong indication" that "some people...are willing to believe anything that sounds plausible and fits their preconceptions about the heroes and villains in politics."

Congressional Republicans Plan Measures To Reverse Some Local DC Policies.

The [Washington Post](#) (1/18, Davis, Portnoy, 11.43M) reports with the coming departure of President Obama, Republicans in Congress are planning "an aggressive push to gut the District's progressive policies," starting with its policies on gun-control, physician-assisted suicide, and "using local funds to provide abortions." Obama, "has stifled" previous efforts, but Republicans "believe Trump will not impede" the measures. While Sen. Chris Van Hollen (D-MD) said Democrats will "be fighting hard to block this effort to make the District of Columbia their personal plaything," Rep. Andy Harris (R-MD) pointed out, "The Constitution gives Congress the right — and obligation — to oversee everything that happens in the District."

High Court Appears Skeptical Of Law Banning Offensive Trademarks.

The [CBS Evening News](#) (1/18, story 10, 2:00, Pelley, 11.17M) reported that on Wednesday "a rock band took the stage at the Supreme Court, hoping to trademark its name." CBS (Crawford) added that "The 'Slants' call their music Chinatown dance rock with a name founder Simon Tam says is a key part of the message." Simon Tam, 'Slants' band leader: "I was ridiculed as a kid for having slanted eyes. Now I'm saying it's something that I can be proud of. It's not something to be ashamed of." The US Patent and Trademark Office "denied the Slants' application saying its name disparages Asian Americans," and "at the Supreme Court, Tam said that violates his First Amendment rights."

The [New York Times](#) (1/18, Liptak, Subscription Publication, 13.9M) reports that the justices "appeared deeply skeptical about the constitutionality of a federal law that

denies protection to disparaging trademarks," and that "almost every member of the court indicated that the law was hard to reconcile with the First Amendment." The Times notes that the court's decision in the case "will probably also effectively resolve a separate one in favor of the Washington Redskins football team." The law "denies federal trademark protection to messages that may disparage people, living or dead, along with 'institutions, beliefs or national symbols,'" and Deputy Solicitor General Malcolm L. Stewart "said the trademark law does not bar any speech, as the Slants remain free to continue to use their name," but Justice Elena Kagan "said that even government programs may not discriminate based on speakers' viewpoints," and Justice Anthony Kennedy "said the law interfered with free expression."

Failed Supreme Court Nominee Garland Returns To Federal Bench.

The [AP](#) (1/18, Gresko) reports that Judge Merrick Garland, who President Obama nominated to the Supreme Court, "made his return to the courtroom on Wednesday to hear cases as a federal appeals court judge, not a Supreme Court justice." Garland, the chief judge of the District of Columbia Circuit, "stopped hearing cases in March after he was nominated to fill the seat of Supreme Court Justice Antonin Scalia, who died in February," but "after Republicans blocked his confirmation, it was announced in mid-December that he'd again begin hearing federal appeals court cases." President-elect Trump "is now expected to announce his own nomination to the court within the two weeks of his inauguration on Friday."

Missouri, New Hampshire Taking Up "Right-To-Work" Bills.

The [AP](#) (1/18, Lieb) reports strengthened Republican majorities in state legislatures are considering efforts "to diminish the power of organized labor" by passing "right-to-work laws" which will be voted on Thursday in the Missouri House and the New Hampshire Senate. Kentucky already enacted a law this month. While it is generally believed that such laws weaken unions, there is some evidence that at least some unions have been able to maintain their membership in states with such laws.

THE BIG PICTURE

Headlines From Today's Front Pages.

Wall Street Journal:

[Donald Trump's Nominees Stick To His Script](#)

[US Races To Finish Probes, Wring Payouts From Firms](#)

[Overhead Bins Not Included: More Airlines Launch No-frills Fares](#)

[Mystery Fungus Sparks NIH Crisis, Imperiling Trials, Patients And Its Boss](#)

New York Times:

[Earth Sets A Temperature Record For The Third Straight Year](#)

[In Farewell, Obama Sets Red Lines That Would Pull Him Back Into Fray](#)

[From Headline To Photograph, A Fake News Masterpiece Student Loan Collector Cheated Millions, Lawsuits Say](#)

Washington Post:

[Congress Moves To Quash DC Laws](#)

[Ethics Concerns Could Derail Cabinet Trio — Or Not](#)

[Two Science Agencies Declare 2016 Hottest Year On Record Suited For A Life Beyond Stonington](#)

[Pick For HHS Defends Trades](#)

Financial Times:

[Goldman And Citigroup Ride Trump Trading Surge](#)

[Indonesian Billionaire A Trump Apprentice Or Conflict-In-Waiting?](#)

[Ross Escalates Trump Trade Criticism Against Beijing](#)

Washington Times:

[Congress Looks To Punish “Sanctuary Campus” Colleges That Protect Illegal Immigrants](#)

[Obama’s Errors Leave Promise To Close Gitmo Unfulfilled](#)

[Trump Inauguration Boycott Grows To Third Of Democratic Caucus](#)

[Obama Assures Nation “We’re Going To Be OK”](#)

[Israel’s Muslims Fear Worst As Netanyahu Eyes Curbs On Mosque Prayer Calls](#)

Story Lineup From Last Night’s Network News:

ABC: Bush Couple Hospitalized; Confirmation Hearing; Obamacare Under Fire; Trump Inauguration; Obama-Manning Pardon; Severe Weather; Italy Earthquake; Texas Gas Explosion; Kidnapped Reunion Interview; Obamas Goodbye.

CBS: Trump Approval Rating; Trump Inauguration; UN Ambassador Nominee; Trump-Russia Dossier; McCain-Trump Transition; Confirmation Hearing; Inauguration Opinions; Bush Couple Hospitalized; Severe Weather; Band Name Supreme Court; Kidnapped Reunion Interview; Obama Final News Conference.

NBC: Bush Couple Hospitalized; Confirmation Hearing; Obama Final News Conference; Hottest Year On Record; Inauguration Opinions; Kidnapped Reunion Interview; Jewish Community Center Bomb Threats; Severe Weather; Baseball Hall Of Fame; Obama Tribute.

Network TV At A Glance:

Confirmation Hearing – 11 minutes, 5 seconds

GHW Bush Couple Hospitalized – 6 minutes, 15 seconds

Inauguration Opinions – 6 minutes, 15 seconds

Trump Inauguration – 4 minutes, 40 seconds

Kidnapped Reunion Interview – 4 minutes, 30 seconds

Obama Final News Conference – 3 minutes, 45 seconds

Severe Weather – 1 minute, 40 seconds

Story Lineup From This Morning’s Radio News

Broadcasts:

ABC: Bush Couple Hospitalized; Trump Inauguration; Obama Final News Conference; Pence Residence LGBT Protest; Student Loan Fraud; Wall Street News.

CBS: Obama Final News Conference; Trump Agriculture Secretary Pick; Confirmation Hearing; Bush Couple Hospitalized; Virginia Convict Execution; Baseball Hall Of Fame; Wall Street News.

FOX: Confirmation Hearing; Inauguration Boycott; Obama Final News Conference; GHW Bush Couple Hospitalized.

NPR: Trump Agriculture Secretary Pick; UN Ambassador Nominee; Bush Couple Hospitalized; Obama Final News Conference; Iraq Mosul Offensive; US Inflation; Auctioned Painting Forgery; Baseball Hall Of Fame.

WASHINGTON’S SCHEDULE

Today’s Events In Washington.

White House:

PRESIDENT OBAMA — No public schedule announced. Final full day of Barack Obama’s presidency.

VICE PRESIDENT BIDEN — No public schedule announced. Final full day of Barack Obama’s presidency.

US Senate: 9:00 AM Republican Sen. Steve Daines hosts Open House ahead of tomorrow’s presidential inauguration Location: Rm 320, Hart Senate Office Bldg., Washington, DC <http://www.daines.senate.gov/> <https://twitter.com/SteveDaines>

9:30 AM Senate Energy and Natural Resources Committee considers Rick Perry to be energy secretary – Nominations hearing considers Rick Perry to be Secretary of Energy * President-elect Donald Trump announced the nomination of the former Texas governor last month Location: Rm 366, Dirksen Senate Office Bldg, Washington, DC <http://energy.senate.gov/public/>

10:00 AM Senate Governmental Affairs subcommittee hearing on improving small business input on federal regulations – Regulatory Affairs and Federal Management Subcommittee hearing on ‘Improving Small Business Input on Federal Regulations: Ideas for Congress and a New Administration’, with testimony from National Federation of Independent Businesses Small Business Legal Center Executive Director Karen Hamed; Small Business Majority Board Member LaJuanna Russell; Action Safety Supply Company President Jerry Hietpas; and National Association of Manufacturers Vice President for Labor, Legal, and Regulatory Policy Rosario Palmieri Location: Rm 342, Dirksen Senate Office Bldg, Washington, DC <http://hsgac.senate.gov/> <https://twitter.com/SenateHSGAC>

10:00 AM Senate Finance Committee considers Steven Mnuchin to be treasury secretary – Nominations hearing considers Steven Mnuchin to be Secretary of the Treasury * President-elect Donald Trump announced the nomination of the former Goldman Sachs partner in November Location: Rm 215, Dirksen Senate Office Bldg, Washington, DC <http://finance.senate.gov>

1:00 PM Senate Dems host forum with Americans who would be hurt by healthcare repeal – Democratic Sens. Debbie Stabenow, Elizabeth Warren, and Patty Murray, plus other senators, host forum with Americans from across the nation who would be hurt by healthcare repeal and the policies supported by Secretary of Health and Human Services-nominee Republican Rep. Tom Price. Witnesses incl people who receive coverage for life-saving drugs under Medicare, who can stay on their parents' insurance until age 26 because of the Affordable Care Act, and who have received mental health coverage under the healthcare law – Ann Serafin of Ferndale, MI, Diane Fleming of Washington, DC, Kanisha Hans of Boston, Alyce Ornella of Harpswell, ME, and Holly Jensen of Cleveland * All 100 senators have been invited to attend Location: Russell Senate Office Bldg, Washington, DC <http://stabenow.senate.gov/> <https://twitter.com/StabenowPress>

3:00 PM Dem Sen. Joe Donnelly holds 'Hoosier Hospitality' event – Democratic Sen. Joe Donnelly hosts 'Hoosier Hospitality' event to welcome constituents picking up tickets for Inauguration Day * Sen. Donnelly holds media availability with Indiana reporters (3:15 PM EST) Location: G50, Dirksen Senate Bldg, Washington, DC www.donnelly.senate.gov <https://twitter.com/SenDonnelly>

No votes scheduled in the Senate Location: Washington, DC <http://www.senate.gov/>

US House: 10:00 AM Michigan Bipartisan Pre-Inaugural Open House – Michigan Bipartisan Pre-Inaugural Open House, celebrating tomorrow's presidential swearing-in ceremony, hosted by Michigan's bipartisan Congressional delegation Location: Rm 1100 Longworth House Office Bldg., Washington, DC www.michiganinaugural2017.com

On recess until 23 Jan.

Other: 10:00 AM Republican National Committee Winter Meeting continues – Republican National Committee Winter Meeting continues with General Session * Event includes vote on the nomination of Michigan Republican Party Chairwoman Ronna Romney McDaniel to chair the RNC, after she was selected for the role by President-elect Donald Trump. If confirmed, McDaniel will replace RNC Chairman Reince Priebus, who is due to become Trump's chief of staff in the White House Location: Omni Shoreham Hotel, 2500 Calvert St., NW, Washington, DC www.gop.com <https://twitter.com/GOP>

12:30 PM U.S. Marshal Service swears in 3,500 law enforcement officers for the inauguration – U.S. Marshal for

the District of Columbia Patrick Burke swears in over 3,500 law enforcement officers from across the country as special deputy U.S. Marshals for tomorrow's 58th U.S. Presidential inauguration Location: DC Armory, 2001 E Capitol St., Washington, DC <http://www.usdoj.gov/marshals/>

2:00 PM Iowa Congressional delegation host reception for Iowans visiting Washington, DC – Republican Sen. Chuck Grassley and other members of the Iowa Congressional delegation host Iowa Delegation Inaugural Reception, for Iowans in Washington, DC, to attend the presidential inauguration Location: Washington, DC <http://grassley.senate.gov/public/> <https://twitter.com/ChuckGrassley>

3:00 PM Supporters of President Obama gather for 'Thanks, Obama' event – 'Thanks, Obama' event, with thousands expected to gather outside the White House to thank outgoing President Barack Obama for his accomplishments and two terms in office * Held before tomorrow's inauguration of President-elect Donald Trump Location: SW Arts Club, 700 Delaware Ave., SW, Washington, DC www.saythanksobama.com <https://twitter.com/thxobamateam>

3:30 PM Donald Trump lays wreath at Arlington National Cemetery and speaks at Welcome Celebration – President-elect Donald Trump and Vice President-elect Mike Pence participate in a wreath-laying at Arlington National Cemetery, Arlington, VA (3:30 PM EST), ahead of their inauguration tomorrow * President-Elect Trump later delivers his first planned remarks in Washington, DC, at the 'Make America Great Again! Welcome Celebration' at the Lincoln Memorial, which includes appearances from Toby Keith, Jon Voight, Jennifer Holliday The Piano Guys, Lee Greenwood, RaviDrums, 3 Doors Down, and The Frontmen of Country, military bands and a fireworks show by Gucci (4:00 PM EST) Location: TBD www.58pic2017.org [#TrumpInaugural](https://twitter.com/trumpinaugural)

4:00 PM Pre-Inaugural 'Make America Great Again! Welcome Celebration' at the Lincoln Memorial – Pre-Inaugural 'Make America Great Again! Welcome Celebration' at the Lincoln Memorial, ahead of the inauguration tomorrow of President-elect Donald Trump and Vice President-elect Mike Pence, with appearances from Toby Keith, Jon Voight, Jennifer Holliday, The Piano Guys, Lee Greenwood, RaviDrums, 3 Doors Down, and The Frontmen of Country (featuring Tim Rushlow, former lead singer of Little Texas, Larry Stewart of Restless Heart and Richie McDonald of Lonestar) * President-elect Donald Trump delivers remarks * Celebration is preceded by Voices of the People, with the DC Fire Department Emerald Society Pipes and Drums, King's Academy Honor Choir, the Republican Hindu Coalition, Montgomery Area High School Marching Band, Marlana Van Hoose, Maury NJROTC Color Guard, Pride of Madawaska, Webelos Troop 177, Northern Middle School Honors Choir,

American Tap Company, South Park and District Pipe Band, Everett High School Viking Marching Band, TwirlTasTix Baton Twirling, and Celtic United Pipes and Drums (10:35 AM EST) Location: Lincoln Memorial, 2 Circle Northwest, Washington, DC www.58pic2017.org
[#TrumpInaugural](https://twitter.com/trumpinaugural)

LAST LAUGHS

Late Night Political Humor.

Jimmy Kimmel: “It’s exciting. We’re two days away from swearing an internet troll in as our 45th President.”

Jimmy Kimmel: “The Trump team has stated repeatedly that they want to avoid a circus-like atmosphere at the inauguration. They’re saving that for the actual presidency itself.”

Jimmy Kimmel: “Betsy DeVos would have made a great secretary of education in 1783 when grizzly bears were a problem.”

Stephen Colbert: “I don’t know if you watched the TV this afternoon, but President Obama held his last press conference today. He talked about the complexities of peace in the Middle East, universal health care, job creation. Pretty boring stuff. And man, I am going to miss being bored.”

Stephen Colbert: “Before he left, he did stun everybody yesterday by commuting the sentence of classified document leaker Chelsea Manning. That was weird. That really surprised me. Because I heard Trump was the one who loved huge leaks.”

Stephen Colbert: “Now the question is, will whistle-blower Edward Snowden now get a pardon? Because today Russia announced it was extending his asylum until 2020. After that, of course, he will face trial under US President Vladimir Putin.”

Stephen Colbert: “Of course, I can understand, Friday’s going to be tough because that is when he gets sworn in, and then Saturday and Sunday he will be googling ‘stuff presidents do.’”

James Corden: “When asked whether or not guns should be allowed in schools, [Betsy DeVos] said that states should decide, citing that, for example, Wyoming schools may need guns to protect themselves from, wait for it, grizzly bears. She knows that the right to ‘bear’ arms isn’t about actual bears, right?”

James Corden: “Yep, it was the hottest year on record. But don’t worry, because this Friday in Washington, DC, hell is going to freeze over.”

Trevor Noah: “If you think about it, Donald Trump is the first famous person to have a wax figure that looks more real than him. I bet Trump’s foundation has already purchased that statue...[Trump] will sneak it into the White House and then go on vacation for four years, just leave it there. And it will do a better job.”

Trevor Noah: [Referring to Education Secretary nominee Betsy DeVos] “Another question I have, how do you put this person in charge of America’s education? It’s like hiring an Amish person to run NASA. ‘All right. Let’s strap some of the horses to the space shutter, and send take it to heaven.’”

Jimmy Fallon: “It’s reported that Donald Trump will use two Bibles when he takes the oath of office. When asked why, he said, ‘In case my hand burns through the first one.’”

Jimmy Fallon: “Did you hear this? After he’s sworn in on Friday, Donald Trump said he’s actually taking the weekend off. Then Obama said, ‘Donald, I think you’re looking at my schedule.’”

Seth Meyers: “President Obama today held the final press conference of his presidency and ended by telling Americans ‘good luck.’ Okay, but how did he say it? Did he say it like mission control says it to an astronaut? Like ‘good luck’? Or like you say it to your buddy leaving the bar with his girlfriend who’s crying and carrying her shoes, like, ‘ooh, good luck.’”

Seth Meyers: “In a newly resurfaced 2015 interview, Donald Trump claimed that he met Russian President Vladimir Putin and that they, quote, ‘got along great.’ That’s right. They were like two peas in a bed.”

Seth Meyers: “Vice President Joe Biden said today that figuring out Donald Trump’s plans for foreign policy is like solving a Rubik’s cube, which is silly. Getting all the colors on different sides is his domestic policy.”

Copyright 2017 by Bulletin Intelligence LLC Reproduction or redistribution without permission prohibited. Content is drawn from thousands of newspapers, national magazines, national and local television programs, radio broadcasts, social-media platforms and additional forms of open-source data. Sources for Bulletin Intelligence audience-size estimates include Scarborough, GfK MRI, comScore, Nielsen, and the Audit Bureau of Circulation. Services that include Twitter data are governed by Twitters’ [terms of use](#). Services that include Factiva content are governed by Factiva’s [terms of use](#). The DHS News Briefing is published seven days a week by Bulletin Intelligence, which creates custom briefings for government and corporate leaders. We can be found on the Web at BulletinIntelligence.com, or called at (703) 483-6100.

2017 MAY -9 AM 10:45
United States Senate
 Washington, DC 20510-1504

May 9, 2017

The Honorable Rod Rosenstein
 Deputy Attorney General
 U.S. Department of Justice
 Washington, DC 20530

The Honorable Daniel R. Coats
 Director of National Intelligence
 Washington, DC 20511

The Honorable John F. Kelly
 Secretary
 U.S. Department of Homeland Security
 Washington, DC 20528

The Honorable James B. Comey, Jr.
 Director
 Federal Bureau of Investigation
 Washington, DC 20535

Dear Deputy Attorney General Rosenstein, Secretary Kelly, Director Coats, and Director Comey:

I am deeply concerned that Russia may be responsible for the recent hacking attack on the campaign of French President-elect Emmanuel Macron, which suggests that Russian President Vladimir Putin is acting with impunity after the lack of accountability for Russia's act of cyber war against the United States during last year's election. Mr. Macron's victory in Sunday's election does not diminish the need for the Trump Administration to take this attack seriously and to work closely with the French government to bring the perpetrators to justice and prevent similar attacks from taking place in the future. I would therefore appreciate a detailed accounting of the Trump Administration's assessment of the attack on the French election and the Administration's response to this attack.

On October 7, 2016, seventeen U.S. intelligence agencies made a damning determination that a foreign adversary deliberately interfered in our election in support of its preferred candidate. The warnings and evidence were overwhelming and a harbinger of future such interference in our elections and those of our Western democratic allies. The conclusions were stark, that Russia would continue to try to undermine confidence in Western democracies and support candidates seen as sympathetic to weakening the Western security alliance. Tragically, a refusal to acknowledge and respond to this serious security threat has resulted in what may have been a Russian attack on the recent French election—and it also leaves our nations at great risk of future such attacks.

Early evidence reportedly points to Russian efforts to hack into the campaign of French President-elect Emmanuel Macron. His campaign called it a "massive and coordinated" hacking operation with the familiar potential to destabilize the election at the last minute. The attacks in France follow a similarly troubling pattern of Russian meddling in recent elections in Germany and the Netherlands and complement ongoing Russian testing and buzzing of Western military defenses in and around Europe. It is of course not surprising that such cyber acts of war continue given the lack of response by this current administration and Congress to the attack on the U.S. election. As one Polish security expert told me recently, the Russians will be watching to see how the United States responds to an attack on its election and will feel emboldened in the absence of any such action—and that appears to be what has happened.

Accordingly, I request responses to the following urgent questions:

- Does the Administration assess that the Russians launched cyber attacks and other acts of disinformation on the French election?
- Has the Administration publicly or privately condemned the Russian actions against the French and other Western elections?
- What has the Administration done to help the French and other Western allies identify and protect against Russian cyber and disinformation campaigns? What is it doing to warn and help allies of such future actions?
- What is the Administration doing to retaliate against such attacks?
- What is the Administration doing to thwart such attacks against future elections in the United States and to help U.S. state governments do the same?
- What is the Administration doing with Congressional leadership to pass appropriate legislation sanctioning Russia for its actions and preventing such attacks in the future?

Quite frankly it is the height of irresponsibility that President Trump still denies Russia's act of cyber war against our election. I fear that this troubling message from the top of the Administration has resulted in inadequate measures to help our allies and our own states protect against such future Russian attacks. Any such continued inaction and denial are a serious abdication of the Administration's urgent national security responsibilities and must be corrected.

Thank you for your time and consideration.

Sincerely,



Richard J. Durbin
United States Senator