(b) (6)

From: NCCIC (b) (7)(E), (b) (7)(F)
Sent: Wednesday, October 12, 2016 5:47 PM
To: (b) (6), (b) (7)(C), (b) (7)(F)
Cc: NCCIC; NCCIC - USCERT; US-CERT Senior Watch Officer; US-CERT operation center
Subject: RE: Contractor For Florida Election System Reportedly Hacked; U.S. Officials Suspect Russian Involvement-UPDATE 3 to MMC IOI #4853-16

Follow Up Flag: Follow up
Flag Status: Completed

(b) (6), (b) (7)(C), (b) (7)(F) or situational awareness.

V/r,

(b) (6), (b) (7)(C), (b) (7)(F)

National Cybersecurity and Communications Integration Center (NCCIC) Duty Officer U.S. Department of Homeland Security

(b) (7)(E), (b) (7)(F)

-----Original Message-----
From: (b) (6)
Sent: Wednesday, October 12, 2016 5:32 PM
Subject: Contractor For Florida Election System Reportedly Hacked; U.S. Officials Suspect Russian Involvement-UPDATE 3 to MMC IOI #4853-16

Location(s): Florida
Federal investigators believe Russian hackers were behind cyberattacks on a contractor for Florida's election system that may have exposed the personal data of Florida voters, U.S. officials briefed on the probe said.

The hack of the Florida contractor comes on the heels of hacks in Illinois, in which personal data of tens of thousands of voters may have been stolen, and one in Arizona, in which investigators now believe the data of voters was likely exposed.

The vendor hack in Florida prompted the FBI last week to coordinate an emergency call with county election supervisors who operate the election system in the perennial battleground state. The name of the vendor that suffered the attack was not immediately known.

A spokeswoman for the Florida Secretary of State said: "We currently have no indication of a Florida-specific issue. The Florida Voter Registration System database is secure. The Department of State does not utilize a vendor for voter

registration services. The Department has in place many safeguards to prevent any possible attempts from being successful."

The various cyberattacks on election registration sites are focused on parts of the U.S. election system that wouldn't affect the votes cast or the vote counts, according to U.S. officials. Instead, the intruders are targeting registration systems.

The FBI, in the coming days, is preparing to provide updated guidance to state elections officials around the U.S. aiming to help them spot suspicious activity on their computer networks. Several states have reported attempted scans of their computer systems, which often is a precursor to a breach.

Traditional Media Sources (some page content may change or not be available over time):
- CNN
-- http://cnn.it/2dKjWp9

The above information summarizes emerging open source reporting that has not been corroborated by official government sources. It is provided to rapidly enhance situational awareness on items of interest to the homeland security enterprise.

(b) (6)

(b) (6)

From: (b) (6), (b) (7)(C), (b) (7)(F) on behalf of NCCIC
Sent: Wednesday, October 12, 2016 5:51 PM
To: (b) (6), (b) (7)(C), (b) (7)(F)
Cc: NCCIC; NCCIC - USCERT
Subject: FW: Contractor For Florida Election System Reportedly Hacked; U.S. Officials Suspect Russian Involvement-UPDATE 3 to MMC IOI #4853-16

(b) (6), (b) (7)(C), (b) (7)(F)

FYI...

(b) (6), (b) (7)(C), (b) (7)(F)

NCCIC Duty Officer (NDO)
National Cybersecurity & Communications Integration Center (NCCIC) Office of Cybersecurity & Communications
National Protection & Programs Directorate Department of Homeland Security Unclassified Phone: (850) 452-6312
(b) (7)(E), (b) (7)(F)

-----Original Message-----
From: SWO (b) (7)(E), (b) (7)(F)
Sent: Wednesday, October 12, 2016 5:44 PM
To: (b) (6), (b) (7)(C), (b) (7)(F)
Cc: NCCIC; NCCIC - USCERT; US-CERT Senior Watch Officer; US-CERT operation center
Subject: RE: Contractor For Florida Election System Reportedly Hacked; U.S. Officials Suspect Russian Involvement-UPDATE 3 to MMC IOI #4853-16

WILCO NDO (b) (6), (b) (7)(C), (b) (7)(F)

Thanks!

(b) (6), (b) (7)(C), (b) (7)(F)

Senior Watch Officer
NPPD/NCCIC/US-CERT
National Cybersecurity & Communications Integration Center (NCCIC) nicholas.cinelli@us-cert.gov
(b) (7)(E), (b) (7)(F)
888-282-0870

-----Original Message-----
From: NCCIC
Sent: Wednesday, October 12, 2016 5:38 PM
To: SWO; SOC

Cc: NCCIC DHS; NCCIC
Subject: FW: Contractor For Florida Election System Reportedly Hacked; U.S. Officials Suspect Russian Involvement-UPDATE 3 to MMC IOI #4853-16

Please add the below information to ticket (b) (7)(E)

V/r,

(b) (6), (b) (7)(C), (b) (7)(F)

NCCIC Duty Officer
National Cybersecurity and Communications Integration Center (NCCIC) U.S. Department of Homeland Security
(b) (7)(E), (b) (7)(F)

-----Original Message-----
From: (b) (6)
Sent: Wednesday, October 12, 2016 5:32 PM
Subject: Contractor For Florida Election System Reportedly Hacked; U.S. Officials Suspect Russian Involvement-UPDATE 3 to MMC IOI #4853-16

Location(s): Florida
Federal investigators believe Russian hackers were behind cyberattacks on a contractor for Florida's election system that may have exposed the personal data of Florida voters, U.S. officials briefed on the probe said.

The hack of the Florida contractor comes on the heels of hacks in Illinois, in which personal data of tens of thousands of voters may have been stolen, and one in Arizona, in which investigators now believe the data of voters was likely exposed.

The vendor hack in Florida prompted the FBI last week to coordinate an emergency call with county election supervisors who operate the election system in the perennial battleground state. The name of the vendor that suffered the attack was not immediately known.

A spokeswoman for the Florida Secretary of State said: "We currently have no indication of a Florida-specific issue. The Florida Voter Registration System database is secure. The Department of State does not utilize a vendor for voter registration services. The Department has in place many safeguards to prevent any possible attempts from being successful."

The various cyberattacks on election registration sites are focused on parts of the U.S. election system that wouldn't affect the votes cast or the vote counts, according to U.S. officials. Instead, the intruders are targeting registration systems.

The FBI, in the coming days, is preparing to provide updated guidance to state elections officials around the U.S. aiming to help them spot suspicious activity on their computer networks. Several states have reported attempted scans of their computer systems, which often is a precursor to a breach.

Traditional Media Sources (some page content may change or not be available over time):
- CNN
-- http://cnn.it/2dKjWp9

The above information summarizes emerging open source reporting that has not been corroborated by official government sources. It is provided to rapidly enhance situational awareness on items of interest to the homeland security enterprise.

(b) (6)

(b) (6)

From: (b) (6)
Sent: Friday, September 22, 2017 5:58 PM
To: NOC.MMC
Subject: 21 U.S. States Notified Of Suspected Russian Hacking Of Voter Systems Ahead Of 2016 Election--MMC IOI #3215-17

Location(s): United States
The federal government on Friday told election officials in 21 states that hackers targeted their systems last year, although in most cases the systems were not breached.

The government told media last year that more than 20 states were targeted by hackers believed to be Russian agents before the 2016 elections. For many states, the calls from the Department of Homeland Security were the first official confirmation of whether their state was targeted.

Federal officials said that in most of the 21 states, the targeting was preparatory activity such as scanning computer systems. The targets included voter registration systems but not vote tallying software. Officials said there were some attempts to compromise networks but most were unsuccessful. Only Illinois reported that hackers had succeeded in breaching its voter systems.

All the states that were targeted have not yet been disclosed, but the list is believed to include Alabama, Arizona, Colorado, Connecticut, Illinois, Iowa, Maryland, Minnesota, Ohio, Oklahoma, Pennsylvania, Virginia, Washington and Wisconsin.

Analyst's Note: The MMC last reported on hacking attempts related to the election on Mar. 3 (See: *FBI Investigating After Millions Of Voter Records Possibly Compromised In Data Breach At Kennesaw State University - Kennesaw, GA--MMC IOI #0963-17)*.

Traditional Media Sources (some page content may change or not be available over time):
- The Associated Press
-- http://bit.ly/2jPnF9s

The above information summarizes emerging open source reporting that has not been corroborated by official government sources. It is provided to rapidly enhance situational awareness on items of interest to the homeland security enterprise.

(b) (6)

From: (b) (6)
Operational Summary--NOC Media Monitoring--4 April 2017
Date: Tuesday, April 4, 2017 1:53:04 AM

MEDIA MONITORING OPERATIONAL SUMMARY (OPSUM)
24 Hour Summary, April 4, 2017

TODAY'S OPSUM COVERS THE FOLLOWING NOC PRIORITIES

- **NOC Priority Items with New Information**
  - Multiple Explosions in Russian Metro System – St. Petersburg, Russia
- **Other Significant Events**
  - Cyber Security
  - Global Terrorism
- **NOC Priority or Numbered Items with Nothing Significant to Report**
  - Southwest Border Events with Homeland Security Implications
  - CBRNE Threats/Incidents Targeting U.S. Interests
  - Mass Migration in the Caribbean with U.S. Homeland Security Implications
  - Global Aviation Cargo Incidents Targeting U.S. Interests
  - Suspicious Activity Reporting:
    - Religious, Cultural and Educational Facilities
    - Postal Shipments
    - National Critical Infrastructure
    - Mass Transit
    - Mass Gatherings and Special Events
  - National Cherry Blossom Parade and Japanese Street Festival – Washington, DC

NOC 0256-17: Multiple Explosions in Russian Metro System – St. Petersburg, Russia

- At least 11 were killed and 39 others injured on Monday following a shrapnel-laden bomb blast in a St. Petersburg metro station Reuters
  - St. Petersburg emergency services initially said that there had been two explosions, but sources later reported a single explosion in a tunnel between stations BBC News
  - A second explosive device, disguised as a fire extinguisher and packed with ball-bearings, was found and disabled at another station
  - The attack is being investigated as an act of terrorism, but no group has yet claimed responsibility

[Back to Top]

Other Significant Events
Cyber Security

- Emirati police in Dubai arrested a group of foreign hackers on Monday that targeted five White House officials Associated Press
  - Police tracked the "African gang" to an apartment in the emirate of Ajman, where they arrested three suspects in possession of "highly confidential information"
    - The suspects had a list of "5 million bank accounts," as well as hacking software and millions of dollars in assets
  - Reports did not identify which White House officials were targeted

- The International Association of Athletics Federations said Monday it suffered a cyberattack that it believes has compromised information about athletes' medical records Associated Press
    - The hacking group Fancy Bear, linked by western governments and security experts to Russian spy agencies, is believed to be behind the attack which occurred in February
        - Fancy Bear hacked into the World Anti-Doping agency database last year, and is additionally believed to be behind cyberattacks during the 2016 U.S. presidential election
    - The hack targeted information concerning applications by athletes for Therapeutic Use Exemptions, used to allow athletes to take certain banned substances for verified medical needs

[Back to Top]

Global Terrorism *(Social Media)*

- *The United Cyber Caliphate, a hacking group with links to the Islamic State of Iraq and the Levant, posted a video over the weekend in which they threatened both the United States and the U.S. president, while also revealing their new "kill list" Twitter [Newsmax]*
    - *In the video the group urges followers to carry out "lone wolf" attacks against those on the list, claiming they will soon publish home addresses Twitter [WTOP - Reporter]*
        - *There are 8,786 names on the list*
    - *Prominent on the list are reportedly well-known figures – including the president*
    - *The group has issued similar hit lists before*

[Back to Top]

(b) (6)

From: (b) (6)
Subject: Operational Summary--NOC Media Monitoring--16 December 2016
Date: Friday, December 16, 2016 2:07:31 AM

MEDIA MONITORING OPERATIONAL SUMMARY (OPSUM)
24 Hour Summary, December 16, 2016

TODAY'S OPSUM COVERS THE FOLLOWING NOC PRIORITIES

- **NOC Priority Items With New Information**
  - Water System Outage – Corpus Christi, TX
  - Significant Winter Weather – Northwest U.S.
- **Other Significant Events**
  - EgyptAir Flight MS804 Crash – Mediterranean Sea
  - Cyber Security
  - Global Terrorism
- **NOC Priority or Numbered Items with Nothing Significant to Report**
  - Southwest Border Events with Homeland Security Implications
  - CBRNE Threats/Incidents Targeting U.S. Interests
  - Mass Migration in the Caribbean with U.S. Homeland Security Implications
  - Global Aviation Cargo Incidents Targeting U.S. Interests
  - Suspicious Activity Reporting:
    - Religious, Cultural and Educational Facilities
    - Postal Shipments
    - National Critical Infrastructure
    - Mass Transit
    - Mass Gatherings and Special Events

NOC 0959-16: Water System Outage – Corpus Christi, TX

- Officials in Corpus Christi on Thursday said a chemical used in asphalt may have contaminated the city's water supply, prompting an advisory against using tap water for everything from drinking to bathing CNN
  - A news release from the city stated the chemical is Indulin AA-86, an asphalt emulsifier
    - Three to 24 gallons of the chemical possibly entered the city's water after an incident in the Corpus Christi industrial district
  - The city of more than 300,000 sent residents an advisory late Wednesday urging them to avoid tap water in "an abundance of caution and until results can confirm water safety"
    - About 100,000 cases of water have been donated to the city for distribution to residents
- The city's news release said a "recent back-flow incident" in the industrial district possibly caused the contamination, but it did not name the industry
  - So far, city testing has been clear, but authorities are still awaiting additional results
    - Late Thursday, officials announced that three locations were declared safe and could resume using tap water: Calallen, Flour Bluff and Padre Island KTRK

[Back to Top]

NOC 0955-16: Significant Winter Weather – Northwest U.S.
California

- Heavy rainstorms and strong wind in Northern California impacted the San Francisco Bay area Thursday KPIX
  - Over 85 flights out of San Francisco International Airport were cancelled, while many more were delayed
  - A winter storm warning went into effect Thursday evening for the mountains, and a wind advisory was previously in effect for the valley and foothills
- Heavy rains and flash floods prompted Marin County officials to activate the county's emergency operations center as multiple roads are closed due to flooding KNTV
  - Crews in the county were helping to evacuate residents from flooded homes in Forest Knolls, Lagunitas and Woodacre
    - A shelter opened at the San Geronimo Community Center in the 6300 block of Sir Francis Drake Boulevard
- A 30-mile stretch of Highway 1 in Northern California was closed in both directions Thursday night after rainy weather caused a rockslide KSBY
  - The highway is closed overnight from Ragged Point to Fullers Point in Monterey County, and crews will assess the situation and work to clear the roadway Friday morning

[Back to Top]

Other Significant Events
NOC 0355-16: EgyptAir Flight MS804 Crash – Mediterranean Sea

- Traces of explosives have been found on some of the victims of the EgyptAir flight from Paris which crashed in May into the Mediterranean Sea, killing 66 Associated Press
  - Due to the findings, a criminal investigation will now begin into the crash of Flight 804
  - No one has claimed to have attacked the plane

[Back to Top]

Cyber Security

- The U.S. agency charged with ensuring that voting machines meet security standards was itself penetrated by a hacker after the November elections, according to a security firm working with law enforcement on the matter Reuters
  - The security firm, Recorded Future, was monitoring underground electronic markets where hackers buy and sell wares and discovered someone offering log-on credentials for access to computers at the U.S. Election Assistance Commission
  - The company officials discovered that a Russian-speaking hacker had obtained the credentials of more than 100 people at the election commission after exploiting a common database vulnerability
    - The hacker was trying to sell information about the vulnerability to a Middle Eastern government for several thousand dollars, but the researchers alerted law enforcement and said Thursday that the hole had been patched
- The Election Assistance Commission said in a statement late Thursday that it had become aware of a "potential intrusion" and was "working with federal law enforcement agencies to investigate the potential breach and its effects"

- "The FBI is currently conducting an ongoing criminal investigation," the statement added
- Researchers do not believe the hacker works for any government or uses sophisticated hacking methods
  - They are confident that the hacker moved to sell his access soon after getting it, meaning that he was not inside the system before election day

- *The FBI has launched an investigation into a massive breach of Yahoo's systems that may have resulted in data theft involving more than one billion user accounts, the White House said Thursday (Social Media) Twitter [USA Today Tech]*
  - *The company had previously acknowledged an extensive compromise of data in a 2014 intrusion that is not believed to be linked to the most recent revelation (Social Media)*
    - *Evidence from that hack, which compromised about 500 million accounts, has been linked to a state-sponsored attacker, though the specific government has not been identified (Social Media)*
- A U.S. citizen living in Moscow was arrested Wednesday after landing at John F. Kennedy International Airport and surrendering to charges that he stole contact information for over 100 million customers of U.S. financial institutions, brokerage firms and financial news publishers, including JPMorgan Chase Associated Press
  - He pleaded not guilty to a 22-count indictment, waiving extradition and asylum in Russia to "responsibly address the charges"
  - Two men had also previously been arrested in Israel and extradited to the U.S. after they allegedly conspired with the suspect to carry out "the single largest theft of customer data from a U.S. financial institution ever"

[Back to Top]

Global Terrorism

Russia

- The Russian Federal Security Service (FSB) says it has arrested four people in and around Moscow and foiled militant attacks allegedly orchestrated out of Turkey Associated Press
  - The FSB reports that officers arrested citizens of the former Soviet republics of Tajikistan and Moldova who were planning a series of high-profile terrorist attacks in Moscow
  - The attacks were reportedly plotted by a Turkey-based militant connected to the Islamic State of Iraq and the Levant

[Back to Top]

(b) (6)

From:	Florida Fusion Center
To:	HQ OSI FIC Cyber Intelligence; Clarke, Stephen; Davenport, Jessica; Wise, Brent
Cc:	Wiggins, Kevin; HQ OSI Supervisors
Subject:	Contractor For Florida Election System Reportedly Hacked; U.S. Officials Suspect Russian Involvement-UPDATE 3 to MMC IOI #4853-16
Date:	Wednesday, October 12, 2016 3:43:53 PM

Please see the below NOC regarding reportedly hacking of Florida election system.

Florida Fusion Center – Intelligence Watch and Warning / FL8567
Florida Department of Law Enforcement
(b) (6)

From: (b) (6)
Sent: Wednesday, October 12, 2016 5:32 PM
Subject: Contractor For Florida Election System Reportedly Hacked; U.S. Officials Suspect Russian Involvement-UPDATE 3 to MMC IOI #4853-16

Location(s): Florida

Federal investigators believe Russian hackers were behind cyberattacks on a contractor for Florida's election system that may have exposed the personal data of Florida voters, U.S. officials briefed on the probe said.

The hack of the Florida contractor comes on the heels of hacks in Illinois, in which personal data of tens of thousands of voters may have been stolen, and one in Arizona, in which investigators now believe the data of voters was likely exposed.

The vendor hack in Florida prompted the FBI last week to coordinate an emergency call with county election supervisors who operate the election system in the perennial battleground state. The name of the vendor that suffered the attack was not immediately known.

A spokeswoman for the Florida Secretary of State said: "We currently have no indication of a Florida-specific issue. The Florida Voter Registration System database is secure. The Department of State does not utilize a vendor for voter registration services. The Department has in place many safeguards to prevent any possible attempts from being successful."

The various cyberattacks on election registration sites are focused on parts of the U.S. election system that wouldn't affect the votes cast or the vote counts, according to U.S. officials.

Instead, the intruders are targeting registration systems.

The FBI, in the coming days, is preparing to provide updated guidance to state elections officials around the U.S. aiming to help them spot suspicious activity on their computer networks. Several states have reported attempted scans of their computer systems, which often is a precursor to a breach.

Traditional Media Sources (some page content may change or not be available over time):
- CNN
-- http://cnn.it/2dKjWp9

The above information summarizes emerging open source reporting that has not been corroborated by official government sources. It is provided to rapidly enhance situational awareness on items of interest to the homeland security enterprise.

(b) (6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

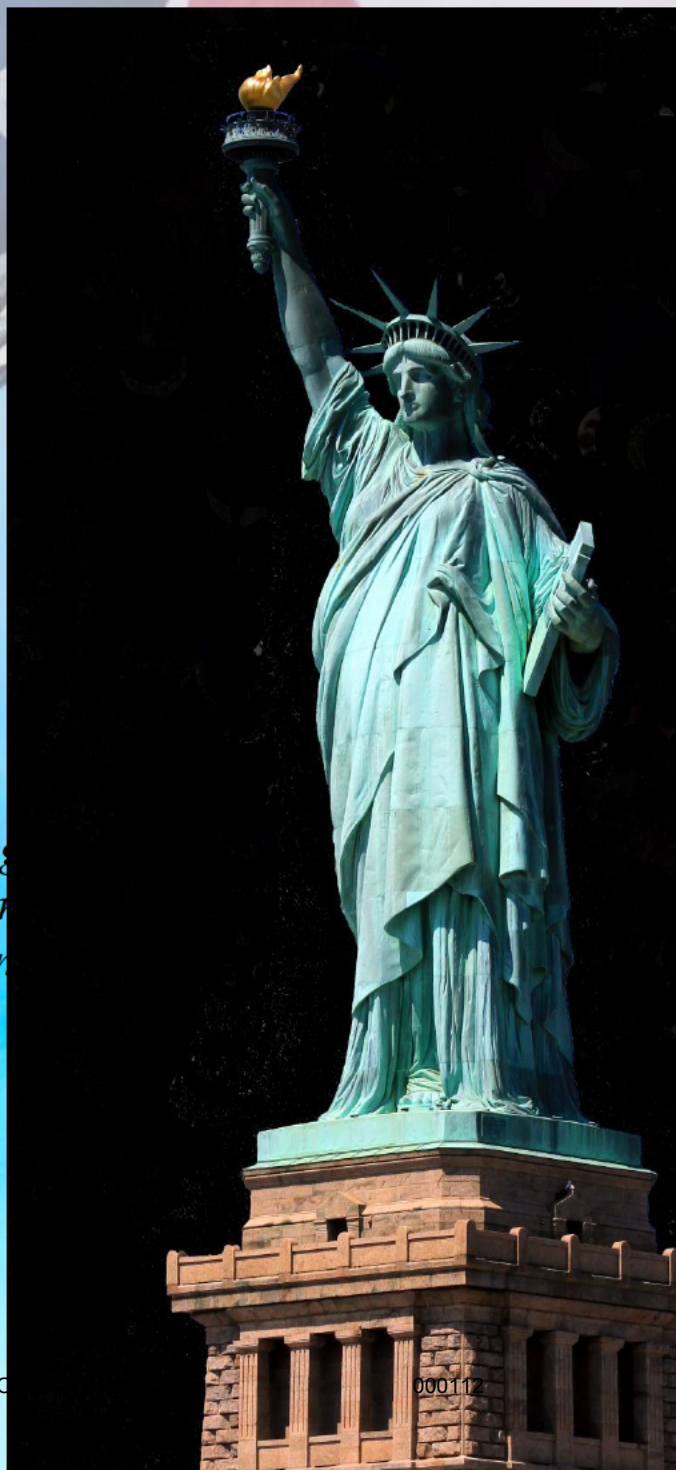
(b) (5)

Homeland Security

Agency Financial Report

Fiscal Year 2016

With honor and integ
safeguard the American
homeland, an



We are DHS

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)