

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION
CENTER,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF
HOMELAND SECURITY,

Defendant.

Civ. Action No. 17-2047

DECLARATION OF JAMES V.M.L. HOLZER

I, James V.M.L. Holzer, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am the Deputy Chief Freedom of Information Act (“FOIA”) Officer for the Department of Homeland Security (“DHS”) Privacy Office (“Privacy Office”).

2. In this capacity, I am the DHS official responsible for implementing FOIA policy across DHS and responding to requests for records under the FOIA, 5 U.S.C. § 552, the Privacy Act, 5 U.S.C. § 552a, and other applicable records access provisions. I have been employed by DHS Privacy in this capacity since May 2016. I previously served as the Director of the Office of Government Information Services within the National Archives and Records Administration, and prior to that I served as the Senior Director of FOIA Operations for DHS.

3. Through the exercise of my official duties, I have become familiar with the background of Plaintiff’s FOIA request dated March 31, 2017. I have also become familiar with the background of this litigation. I make the statements herein based on my personal knowledge, as well as on information that I acquired while performing my official duties.

4. The DHS Privacy Office Disclosure team is responsible for receiving, tracking, processing, and closing all FOIA requests received by the DHS Privacy Office. The DHS

1 Privacy Office FOIA staff processes initial FOIA and Privacy Act (PA) requests to the Office of
2 the Secretary (including the Military Advisor's Office), Office of the Citizenship and
3 Immigration Services Ombudsman, Countering Weapons of Mass Destruction Office, Office of
4 the Executive Secretary, Office of Partnership and Engagement, Management Directorate, Office
5 for Civil Rights and Civil Liberties, Office of Operations Coordination, Office of Strategy,
6 Policy, and Plans, Office of the General Counsel, Office of Legislative Affairs, and Office of
7 Public Affairs. This team is also responsible for engaging with the Components on the proper
8 handling and processing of all FOIA transfers and referrals to DHS Privacy Office. As of the
9 Fiscal Year 2020, the DHS Privacy Office Disclosure team is also responsible for processing
10 initial FOIA and PA requests for the Cybersecurity and Infrastructure Security Agency (CISA)
11 as well as the Office of Biometric Identity Management, the Office of Science & Technology
12 and other DHS Headquarters components.

14 5. On March 31, 2017, Plaintiff submitted a FOIA request to DHS. On April 6,
15 2017, Plaintiff's request was referred to the DHS National Protection and Programs Directorate
16 (NPPD), which is now CISA.

18 6. At the time Plaintiff submitted its FOIA request, CISA—then NPPD—processed
19 its own FOIA requests. Plaintiff's FOIA request was assigned request number 2017-NPFO-
20 0430. After Plaintiff filed its Complaint, CISA's FOIA operations were consolidated within the
21 Privacy Office.

22 7. CISA processed and released some responsive records in this case, and the parties
23 have worked to narrow the issues in dispute.

24 8. After reviewing the records CISA had produced as well as a CISA-provided draft
25 *Vaughn* Index of records withheld in full that were not drafts or e-mail chains, Plaintiff requested
26

27

28

1 that CISA reprocess four categories of records, totaling 16 documents, that were previously
2 withheld in full. These four categories of records were: (1) Documents concerning contacts
3 between the DHS and State Election Officials; (2) Election Task Force meeting minutes; (3)
4 Documents about risk characterizations and analysis reports on Russian interference;¹ and (4)
5 Incident reports and vulnerabilities in election systems.

6 9. On February 14, 2020, CISA informed EPIC that it had reprocessed the
7 documents identified by Plaintiff. CISA released three pages in full and withheld five pages in
8 part and 80 pages in full pursuant to Exemptions 5, 6, and 7(E). CISA explained that six pages
9 required further consultation with another agency. On February 28, 2020, the DHS informed
10 EPIC that it had completed consultation of the DHS/FBI Joint Analysis Report and released that
11 report in full.
12

13 10. Based on its review, Plaintiff stated in a Joint Status Report filed in this action on
14 February 28, 2020 (ECF No. 23) that the only issues remaining in dispute are the (b)(5) and
15 (b)(7)(E) exemption claims and the segregability determinations as to the 13 of the 16
16 reprocessed documents not produced in full. Plaintiff stated that it agreed not to challenge the
17 withholding of any other documents, nor will it challenge the searches conducted by CISA.
18

19 11. One of the documents not released in full contained only applications of
20 Exemption (b)(6). Plaintiff has indicated that it does not intend to challenge CISA's application
21 of Exemption (b)(6), and thus the exemption claims of this document (document number NPPD
22 001702) is not subject to this dispute. Therefore, 12 of the 16 reprocessed documents remain in
23 dispute.
24

25
26 ¹ The third category of documents that Plaintiff identified included two documents that have been released and thus
27 are no longer the subject of Plaintiff's challenge. The remaining document in this category is a document entitled
28 "Election Infrastructure Cyber Risk Characterization," and DHS is referring to this document by its title *infra*.

1 12. The purpose of this declaration is to describe the basis for withholding the
2 contested portions of the records released by CISA.

3 **CISA Withholdings**

4 13. After review of the responsive records, CISA determined that the records were
5 exempt pursuant to FOIA Exemptions (b)(5), (b)(6), and (b)(7)(E).
6

7 14. After receiving and reviewing all of CISA's productions, Plaintiff indicated,
8 through counsel, its intent to challenge portions of CISA's withholdings. Plaintiff further
9 indicated that it does not intend to challenge CISA's application of Exemption (b)(6). This
10 declaration, and the attached *Vaughn* index describe the reasons for withholding the exempt
11 records that Plaintiff has challenged.²
12

13 **Exemption 5**

14 15. CISA withheld each of the twelve documents under FOIA Exemption (b)(5).
15 FOIA Exemption (b)(5) protects "inter-agency and intra-agency memorandums or letters which
16 would not be available by law to a party other than an agency in litigation with the agency." 5
17 U.S.C. § 552(b)(5).

18 16. The deliberative process privilege is intended to protect the decision-making
19 processes of Executive Branch agencies from public disclosure in order to enhance the quality of
20 agency decisions and to encourage and facilitate candid discussions among Executive Branch
21 employees. Disclosure of deliberative process records would severely hamper the efficient day-
22 to-day workings of the Department, as individuals would no longer feel free to candidly discuss
23

24 _____
25 ² After CISA processed and made productions of the documents located pursuant to its search, CISA located one
26 additional document while finalizing the *Vaughn* index. This additional document is a slightly updated version of a
27 document withheld in full pursuant to Exemptions (b)(5) and (b)(7)(E) (document number NPPD 000967). The
28 additional document was located in an employee's email archive and is dated November 17, 2016. Exemptions
(b)(5) and (b)(7)(E) apply to the additional document in the same manner as the version processed and included in
CISA's production.

1 their ideas, strategies, and advice in written communications. Department operations would be
2 hampered because the disclosure of such preliminary assessments and opinions would make
3 employees contributing to pre-decisional deliberations much more circumspect in providing their
4 written views. This lack of candor will seriously impair the Department's ability to foster the
5 forthright internal discussions necessary for efficient and proper decision-making. Agency
6 decision-making is best enhanced when employees are able to freely discuss and debate their
7 views and are not tempered by considerations of public release of their discussions and internal
8 pre-decisional deliberations.
9

10 17. Executive Branch staff prepare documents to brief, or to prepare to brief, senior
11 leadership officials on pending questions on various legal and policy points. These documents
12 are prepared in advance of an agency decision on these matters, and are for the purpose of
13 informing, advising, deliberating, and/or recommending that the decisionmaker take (or not to
14 take) a certain course of action. Such briefing materials are therefore pre-decisional, inasmuch
15 as they precede the decision being advised on, and do not embody final agency action. The
16 drafters of these briefing materials attempt to succinctly summarize particular events, identify
17 important issues and questions, provide key background information, and may provide a
18 recommendation — all in order to facilitate an official's decision on the matter. Throughout this
19 process, the drafters necessarily review and analyze the underlying circumstances and potential
20 issues arising on the topic at hand, and then selectively craft materials to reflect the information
21 and/or guidance that, in their judgment, is necessary and integral to aiding the decisionmaker's
22 determination on the question at hand. The documents reflect the drafters' preliminary view of
23 the facts and their relevancy. The decision to include or exclude certain information in or from
24 analytical documents is therefore itself an important part of the deliberative process. The
25
26
27
28

1 agency's senior officials rely heavily on the creation of such briefing materials so that they can
2 guide and/or make a determination on the substance of the many legal and policy issues being
3 considered by the agency every day in individual offices. CISA's senior leaders are responsible
4 for carrying out CISA's mission, which includes identifying and addressing the most significant
5 risks to critical infrastructure. The deliberative documents were provided to brief CISA's senior
6 official aid those officials in making decisions regarding the assessment and management of
7 risks to critical infrastructure. Thus, disclosure of these documents would foreseeably harm the
8 decision-making process of the agency's senior leadership by inhibiting the flow of staff-level
9 views and assessments.
10

11 18. As described in detail in the attached *Vaughn* index, CISA applied Exemption
12 (b)(5) to protect privileged deliberative information contained within the requested records from
13 disclosure, because the information consists of the thoughts, opinions, and pre-decisional
14 impressions of agency employee and non-final sensitive information gathered to inform agency
15 decision-making. These materials were used to brief or prepare to brief agency leadership
16 regarding election infrastructure security. In each category of documents that Plaintiff requested
17 CISA reprocess, CISA identified deliberative, pre-decisional information that is properly
18 withheld pursuant to Exemption (b)(5).
19

20 19. Contacts between the DHS and State election officials: In the documents
21 concerning contacts between the DHS and State Election Officials, CISA withheld employees'
22 frank summaries of meetings with State election infrastructure officials that contained
23 recommendations, emphasized points, and key areas of concern. The documents further contain
24 staff assessments of the meetings and engagements with certain State officials and agency staff's
25 then-current tracking and understanding of the status of vulnerabilities in certain States' election
26
27
28

1 infrastructure, along with recommendations for future action as a result of those assessments and
2 understanding. The assessments are not final and reflect substantial uncertainty. The documents
3 were used only internally within DHS and were provided to agency leadership on an on-going
4 basis to help leadership track the current status of staff engagement with State officials and to aid
5 leadership in making decisions regarding prioritizing time and resources to meet emerging needs
6 related to the agency's election infrastructure security activities. Release of the documents
7 would foreseeably harm the agency by inhibiting agency staff's ability to communicate frank,
8 current, non-final assessments to agency leadership, which would harm agency leadership
9 decision-making by depriving them of developing information. Further, release of non-final
10 information would give the public an erroneous understanding of the basis for agency decisions.
11

12 20. Election Tasks Force Meeting Minutes: In the Election Task Force meeting
13 minutes documents, CISA withheld the deliberative information documented in the meeting
14 minutes, which were shared only with the interagency partners on the Task Force. The Task Force
15 advised and provided information to the Secretary of Homeland Security, the Under Secretary of
16 NPPD, and other agency leadership regarding election security. The Task Force was a temporary
17 mechanism and was disbanded when the Under Secretary of NPPD determined that its functions
18 could be operated within NPPD offices. The Task Force meeting minutes contain reports, status
19 updates and assessments from individual Task Force members in furtherance of the Task Force's
20 goal of assessing risk to election infrastructure. The Task Force meeting minutes also reflect
21 potential recommendations that the Task Force would make to agency leadership to inform
22 planning, resourcing, and prioritization of DHS's election infrastructure security efforts.
23 Disclosure of the information would have a chilling effect on the deliberative discussions of
24 meeting of agency task forces, which study particular issues and provide recommendations to
25
26
27
28

1 agency leadership. Chilling this communication between agency employees and between agency
2 staff and leadership would foreseeably harm the agency by undermining the agency's ability to
3 perform its duties. CISA depends on the ability of its employees to offer candid ideas and opinions
4 to agency decision-makers and to each other without the fear of public exposure; to curtail this
5 process would be detrimental to CISA and all government entities.

6 21. Election Infrastructure Cyber Risk Characterization Report: CISA applied
7 Exemption (b)(5) to protect pre-decisional deliberative information in a report concerning
8 election infrastructure cyber risk characterization prepared by CISA's Office of Cyber and
9 Infrastructure Analysis for wider Departmental leadership consideration and to aid in decisions
10 regarding areas where the agency could best help mitigate risk to election systems. The
11 document was prepared for internal purposes only and contains select, non-final, in-process
12 assessments and characterizations of election infrastructure vulnerabilities. The office provided
13 the assessments and characterizations to support DHS's planning to enhance security of election
14 infrastructure and to aid decisions regarding areas where the agency could best help mitigate risk
15 to election systems, and selected the assessments and characterizations that in the office's
16 judgment were most relevant to leadership planning at that time. . Disclosure of the information
17 would foreseeably harm the agency's ability to assemble and communicate such information for
18 leadership planning. Further, disclosing non-final assessments of vulnerabilities could mislead
19 the public as to the reasons and basis for later agency actions and final assessment of facts.

22 22. Incident Reports: In the incident reports about vulnerabilities in election systems,
23 CISA applied Exemption (b)(5) to protect non-final assessments of election infrastructure
24 defense, agency staff analysis and recommendations, and coordination plans. The reports
25 contain unverified, preliminary information, and timelines of on-going agency staff engagements
26
27
28

1 and discussions, which were documented for and provided to agency leadership for leadership's
2 situational awareness and oversight to aid in planning of election infrastructure security efforts.
3 The reports also contained preliminary findings provided to another federal agency along with
4 recommended actions for that agency's consideration. Disclosure of these reports would
5 foreseeably harm CISA's ability to communicate clearly and frankly with other federal partners
6 and would harm CISA staff's ability to provide transparent communication and assessments to
7 CISA leadership. Disclosure of non-final reports would also mislead the public by releasing
8 non-final assessments of sensitive information.
9

10 **Exemption 7(E)**

11 23. DHS withheld eight records pursuant to FOIA Exemption (b)(7)(E).³ Exemption
12 7(E) affords protection to all documents "compiled for law enforcement purposes" that "would
13 disclose techniques and procedures for law enforcement investigations or prosecutions, or would
14 disclose guidelines for law enforcement investigations or prosecutions if such disclosure could
15 reasonably be expected to risk circumvention of the law."
16

17 24. CISA applied FOIA Exemption (b)(7)(E) to protect documents compiled for law
18 enforcement purposes relevant to the CISA's efforts to secure the Nation's election system
19 infrastructure. The Secretary of Homeland Security's responsibilities relating to infrastructure
20 security include accessing, receiving, and analyzing law enforcement information in order to
21 identify and assess the nature and scope of terrorist threats.⁴ DHS's responsibilities further
22 include making recommendations on protective measures for critical infrastructure in
23

24
25 ³ Three documents related to contacts between the DHS and State Election Officials (NPPD 000419; NPPD 000944;
26 NPPD 000967); the Election Infrastructure Cyber Risk Characterization Report (NPPD 0000926 – 000942) and four
27 incident reports (NPPD 000962; NPPD 000963 – 000966; NPPD 001115 – 001119; NPPD 001095 – 001106). As
28 noted above, CISA located one additional document that is an updated version of document NPPD 000967. FOIA
exemption 7(E) would apply equally to that additional document as it does to NPPD 000967.

⁴ See 6 U.S.C. § 652(e)(1)(A).

1 coordination with other Federal agencies and with State, local, tribal, and territorial government
2 agencies.⁵ As a Component of DHS, CISA has responsibility and authority for overseeing
3 critical infrastructure protection, including election infrastructure. The documents CISA has
4 protected pursuant to FOIA exemption (b)(7)(E) were compiled pursuant to these responsibilities
5 and used for the purposes of assessing threats to election system infrastructure and making
6 recommendations for the protection thereof. These documents contain information about
7 coordination with other Federal law enforcement agencies and State government representatives
8 responsible for election infrastructure security.
9

10 25. Here, release of information describing the steps CISA takes to assess and
11 mitigate risks to election systems would divulge nonpublic procedures to safeguard election
12 system infrastructure and to detect possible interference. Were the public made aware of the
13 procedures CISA uses to assess and respond to cybersecurity incidents on or vulnerabilities in
14 States' election systems, it could allow bad actors who intend to disrupt the Nation's election
15 infrastructure to evade CISA's detection techniques and circumvent its mitigation procedures,
16 which would put States' election systems at greater risk.
17

18 26. Because CISA's election system security efforts include assessing where risks are
19 highest and which States may be subject to greater vulnerabilities, disclosure of CISA's
20 assessments would enable bad actors to target certain States or areas, significantly increasing
21 their risks. Moreover, because some of the documents contain discussions of specific incidents,
22 release of the information would alert those who attempted to compromise the election
23 infrastructure of the degree to which their actions were detected. This may encourage those
24
25
26

27 ⁵ See 6 U.S.C. § 652(e)(1)(C).
28

1 actors to either try the same measures again if they perceive they were not fully detected or to try
2 other means that they believe would more effectively evade detection.

3 27. The Election Infrastructure Cyber Risk Characterization Report contains detailed
4 information concerning assessment of States' election infrastructure vulnerabilities, risks of
5 cyber intrusion and mitigation possibilities.⁶ The report describes in detail nonpublic techniques
6 and procedures that the agency uses to make such assessment. Release of this information would
7 allowing targeting of states perceived to have higher risk factors or provide models for disrupting
8 elections systems.
9

10 28. The incident reports contain nonpublic assessments and tests the agency uses to
11 detect and analyze State election infrastructure vulnerabilities. For example, one chart shows
12 reports of tests of State election infrastructure and vulnerability assessments, which were not
13 made public.⁷ Disclosure of the test techniques and results would reveal the technique and
14 procedures used to access and respond to States' infrastructure vulnerabilities. Disclosure of
15 such technique would risk rendering the techniques and procedures ineffective.
16

17 29. Charts of contacts between NPPD and State Election Officials contain
18 information on the nonpublic techniques and procedures the agency uses to assess and address
19 risks to and vulnerabilities in States' election infrastructure. For example, one chart contains
20 assessments of cyber hygiene vulnerabilities in States' election infrastructure and NPPD's
21 coordination with States regarding protective measures.⁸ Release of this information would put
22 such techniques and procedures at risk of being undermined or rendered ineffective and allow
23 targeting of States with perceived greater risk factors.
24

25
26 ⁶ See NPPD 000926-000942.

27 ⁷ See NPPD 000963-000966.

28 ⁸ See NPPD 000967.

Segregability

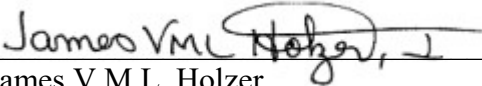
1
2 30. CISA performed a line-by-line review of each CISA record responsive to
3 Plaintiff FOIA request, and determined that all segregable information has been released.

4 31. DHS also conducted a record-by-record review of each CISA withholding under
5 the exemptions at issue here and determined that it reasonably foresees that release would be
6 harmful to its deliberative process and to its law enforcement techniques and procedures, for the
7 reasons stated above in paragraphs 15-29.

8 32. All of the information withheld has been carefully reviewed to ensure that the
9 maximum release to Plaintiff and all releasable information has been released pursuant to the
10 FOIA. All information was either fully covered by one or more FOIA exemptions or any non-
11 exempt information was so intertwined with exempt material that no information could be
12 reasonably segregated for release. The withheld information, if released, would reveal the
13 information sought to be protected by the exemption(s) claimed. Accordingly, there is no
14 additional segregable information that can be released to Plaintiff.
15
16

17 Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the
18 foregoing is true and correct.

19 Dated the 15th day of May, 2020

20
21 
22 James V.M.L. Holzer
23 Deputy Chief FOIA Officer
24 DHS Privacy Office
25 U.S. Department of Homeland Security
26
27
28

EPIC v. DHS Vaughn Index Case No. 1:17-cv-2047						
Bates Range	Page Number	Release Document Name	Description of Document	Date	Exemptions Applied	Explanation of Withholdings
Election Task Force Meeting Minutes						
NPPD 000505 - NPPD 000507 NPPD 000394 - NPPD 000400	2-4 82-88	"Election Task Force Minutes"	Meeting Minutes	Oct. 25, 2017 Oct. 11 & 12, 2017	(b)(5) - deliberative process	CISA applied FOIA exemption (b)(5) to protect minutes of a deliberative task force meeting, discussion of task force priorities, status updates and assessments from individual members, and what recommendations to provide to agency leadership. The task force advised and provided information to the Secretary of Homeland Security, the Under Secretary of NPPD, and other agency leadership regarding election security. The task force was a temporary mechanism and was disbanded when the Under Secretary of NPPD determined that its functions could be operated within NPPD offices. The task force meeting minutes contained reports, status updates and assessments from individual task force members in furtherance of the Task Force's goal of assessing risk to election infrastructure. The minutes were shared only within the interagency partners on the task force. The task force meeting minutes reflected potential recommendations that the task force would make to agency leadership to inform planning, resourcing, and prioritization of agency infrastructure security efforts. Disclosure of the information would have a chilling effect on the free deliberative discussions of agency task force meetings.
Contacts Between DHS and State Election Officials						
NPPD 000351- NPPD 000360 NPPD 000401 - NPPD 000410	9-18 24-33	"Weekly Summary for Meetings with Elections Infrastructure Officials"	Excel spreadsheets		(b)(5) - deliberative process	CISA applied FOIA exemption (b)(5) to protect internal summaries of meetings with state election infrastructure officials, including key discussion points, areas of concern, and recommendations for follow-up and what information to raise to agency leadership. The information is pre-decisional and includes recommendations for leadership action related to election security efforts. Disclosure of the information would harm the ability of agency staff to frankly document notes of meetings and provide recommendations based on those meetings for agency leadership.
NPPD 000419 NPPD 000944	46 50		One spreadsheet describing engagement with 22 states by NPPD and one spreadsheet describing engagement with 3 states		(b)(5) - deliberative process; (b)(7)(E)	CISA applied FOIA exemption (b)(5) to protect deliberative, non-final information documented in this spreadsheet. The internal document contains frank assessments of NPPD's then-current engagement with certain states, NPPD staff's understanding of the status of vulnerabilities in the states' election infrastructure, and recommendations for future actions. The assessments reflect substantial uncertainty and were not final. The chart was compiled in preparation for briefing staff's leadership to aid in leadership decisions regarding time and resource prioritization. Release of the deliberative information would harm agency staff's ability to compile frank, non-final assessments for leadership awareness. Release of the non-final and uncertain assessments would be misleading to the public. CISA applied FOIA exemption (b)(7)(E) to protect the nonpublic techniques and procedures used to assess state election infrastructure vulnerabilities and steps that CISA would take with states to address the vulnerabilities. The records were compiled for law enforcement purposes as part of the agency's responsibilities for protecting critical infrastructure and coordinating with State government agencies. Disclosure of this information would harm CISA's ability to effectively assess and address such vulnerabilities.

<p>NPPD 000967 Additional document 1</p>	<p>63</p>	<p>"State Outreach Status - DHS Election Infrastructure Campaign"</p>	<p>Chart of the status of NPPD's outreach to states regarding risk vulnerability and cyber hygiene assessments for states' election infrastructure</p>	<p>Originally processed document undated Additional document dated Nov. 17, 2016</p>	<p>(b)(5) - deliberative process; (b)(7)(E)</p>	<p>CISA applied exemption (b)(5) to protect deliberative information in this interim progress report chart, which was not finalized. The chart was used as an internal tracking document used to provide leadership with status updates and progress reports, which agency leadership would then use to make determinations regarding resource allocations. Release of the information would be misleading, as the information is not final or fully verified. Additionally, releasing the information would inhibit agency staff's ability to provide non-final assessments and updates to agency leadership. CISA notes that the additional document located after processing all documents found in the search contains minor updates from the originally processed document. These updates are indicative of a working document that contained preliminary and interim information.</p> <p>CISA applied FOIA exemption (b)(7)(E) to protect the nonpublic techniques and procedures CISA uses to assess risk and cyber hygiene vulnerabilities in states' election infrastructure. The chart was compiled for law enforcement purposes to assess threats to election infrastructure and coordination with States regarding protective measures. Release of this information would put such techniques and procedures at risk of being undermined or rendered ineffective and allow targeting of states with perceived greater risk factors.</p>
<p>Election Infrastructure Cyber Risk Characterization</p>						
<p>NPPD 000926 - NPPD 000942</p>	<p>64-80</p>	<p>"Election Infrastructure Cyber Risk Characterization"</p>	<p>NPPD Office of Cyber and Infrastructure Analysis record, documenting internal assessment of the election infrastructure and potential cyber vulnerabilities</p>	<p>Sept. 2016</p>	<p>(b)(5) - deliberative process; (b)(7)(E)</p>	<p>CISA applied FOIA exemption (b)(5) to protect pre-decisional, deliberative information provided by one office within the agency, the Office of Cyber and Infrastructure Analysis, for wider internal departmental leadership consideration. The office provided its non-final, in-process assessments and characterizations of select election infrastructure vulnerabilities and likelihood of cyber intrusions that could disrupt elections. The office provided the assessments and characterizations to support DHS's planning to enhance security of election infrastructure and to aid decisions regarding areas where the agency could best help mitigate risk to election systems, and selected the assessments and characterizations that in the office's judgment were most relevant to leadership planning at that time. Disclosure would harm agency office's ability to create and provide such products to inform leadership planning.</p> <p>CISA applied FOIA exemption (b)(7)(E) to protect detailed, nonpublic law enforcement information concerning assessments of states' election infrastructure vulnerabilities, risks of cyber intrusion, and mitigation possibilities. The document, compiled for law enforcement purposes, assesses the systems, assets, and networks most critical to security and resilience of election systems and assesses factors that increase or decrease risk. The document describes in detail the techniques and procedures that the agency uses to make such assessments, the release of which would harm their continued use. Release of the information could allow targeting of states with perceived higher risk factors or provide models for disrupting election systems.</p>
<p>Incident Reports about Vulnerabilities in Election Systems</p>						

<p>NPPD 000962</p>	<p>1</p>		<p>Untitled report sent by the National Cybersecurity and Communications Integration Center (NCCIC) to restricted recipients regarding actions to be taken in advance of Election Day; includes an incident summary and state vulnerability scanning and assessments</p>		<p>(b)(5) - deliberative process; (b)(7)(E)</p>	<p>CISA applied FOIA exemption (b)(5) to protect deliberative information contained in the report regarding plans to coordinate intra- and inter-agency efforts ahead of Election Day. The report reflects assessments about which no final decision had been made, including in-progress scanning assessments and coordination planning. Disclosure of this information would be harmful to CISA in making deliberations open to the public and chilling the discussion needed for thorough and effective coordination with the agency's partners. Disclosure would may also mislead the public by providing non-final assessment information.</p> <p>CISA applied FOIA exemption (b)(7)(E) to protect nonpublic reports of tests of state election infrastructure and vulnerability assessments. The report was compiled for law enforcement purposes in furtherance of the agency's responsibilities to protect election infrastructure. Disclosure of the test techniques and results would reveal techniques and procedures CISA used to assess and respond to states' election infrastructure vulnerabilities, the release of which would risk rendering the techniques and procedures ineffective.</p>
<p>NPPD 000963 - NPPD 000966</p>	<p>5-8</p>	<p>"Election Related State Incidents"</p>	<p>List of election related incidents in chart form</p>		<p>(b)(5) - deliberative process; (b)(7)(E)</p>	<p>CISA applied FOIA exemption (b)(5) to protect deliberative and predecisional interagency analysis, recommendations and assessments regarding network and election infrastructure defense. This document charts unverified, non-final information as the agency received it, and thus the information would be misleading if released. The chart was used to brief agency leadership on election-related incidents and investigations, for the purpose of aiding leadership's planning efforts. Disclosure of the information would inhibit the agency staff's ability to communicate effectively and transparently with leadership.</p> <p>CISA applied FOIA exemption (b)(7)(E) to protect reports of tests of state election infrastructure and vulnerability assessments. The reports were compiled for law enforcement purposes pursuant to the agency's responsibilities to protect critical infrastructure and were not made public. Disclosure of the test techniques and results would reveal techniques and procedures CISA used to assess and respond to states' election infrastructure vulnerabilities, the release of which would risk rendering the techniques and procedures ineffective. Disclosure would also risk entities not reporting to the agency in the future if their information is released.</p>
<p>NPPD 001115 - NPPD 001119</p>	<p>19-23</p>	<p>"National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Readiness Teams (US-CERT) Preliminary Digital Media Analysis Report regarding cyber incident"</p>	<p>Preliminary Digital Media Analysis Report prepared for another federal agency(document marked unclassified//FOR OFFICIAL USE ONLY)</p>	<p>Sept. 2, 2016</p>	<p>(b)(5) - deliberative process; (b)(7)(E)</p>	<p>CISA applied FOIA exemption (b)(5) to protect preliminary findings provided to another federal agency and recommendations for how to mitigate the issues identified in the report. CISA provided the agency with findings and recommended actions for the other agency's deliberation and potential implementation. Disclosure of the information would harm CISA's ability to provide clear assessments of cyber incidents and frank recommendations for other federal agencies.</p> <p>CISA applied FOIA exemption (b)(7)(E) to protect the nonpublic techniques and procedures CISA uses to analyze cyber incidents and the recommendations the agency has for mitigating vulnerabilities. The NPPD NCCIC compiled this report for law enforcement purposes pursuant to the agency's responsibilities to protect critical infrastructure and to coordinate with other Federal agencies regarding recommendations for protective measures. Disclosure of this information would risk circumvention of these techniques and procedures, and render them ineffective.</p>

<p>NPPD 001095 - NPPD 001106 Duplicated in NPPD 001864 - NPPD 001875</p>	<p>34-45 Duplicate at 51-62</p>	<p>"Timeline (July 28, 2016 through August 31, 2016) of emails/incident reports received by NPPD/NCCIC and responses pertaining to election security"</p>	<p>Timeline (July 28, 2016 through August 31, 2016) of emails/incident reports received by NPPD/NCCIC and responses pertaining to election security</p>	<p>July 28 - Aug. 31, 2016</p>	<p>(b)(5) - deliberative process; (b)(7)(E)</p>	<p>CISA applied FOIA exemption (b)(5) to protect deliberative information in this document, which provides a timeline of agency staff engagements and discussions, including emails, calls, briefings, and incident reports to the NCCIC pertaining to election security. The document was created by agency staff to provide agency leadership a tool for oversight and awareness of staff's work to assist leadership planning and resource allocation decisions. The document includes select facts, summaries of deliberative exchanges between agency staff, staff assessments of certain exchanges with outside parties, and recommendations for next steps. Disclosure of the information would chill the open communication between agency staff and agency leadership, and would inhibit agency leadership oversight of staff engagements.</p> <p>CISA applied FOIA exemption (b)(7)(E) to protect descriptions of CISA's nonpublic techniques and procedures for detecting and mitigating threats to election systems. The information was compiled for law enforcement purposes pursuant to the agency's role in protecting election infrastructure. Disclosure of this information would jeopardize CISA's abilities to effectively detect and mitigate risks to the election infrastructure.</p>
---	--	---	---	--------------------------------	---	---