DECLARATION OF JAMES V.M.L. HOLZER

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


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

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

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

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

8. After reviewing the records CISA had produced as well as a CISA-provided draft *Vaughn* Index of records withheld in full that were not drafts or e-mail chains, Plaintiff requested
that CISA reprocessed four categories of records, totaling 16 documents, that were previously
withheld in full. These four categories of records were: (1) Documents concerning contacts
between the DHS and State Election Officials; (2) Election Task Force meeting minutes; (3)
Documents about risk characterizations and analysis reports on Russian interference;\(^1\) and (4)
Incident reports and vulnerabilities in election systems.

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

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

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

---

\(^1\) The third category of documents that Plaintiff identified included two documents that have been released and thus
are no longer the subject of Plaintiff’s challenge. The remaining document in this category is a document entitled
“Election Infrastructure Cyber Risk Characterization,” and DHS is referring to this document by its title \textit{infra}. 
12. The purpose of this declaration is to describe the basis for withholding the contested portions of the records released by CISA.

**CISA Withholdings**

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

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

**Exemption 5**

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

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

---

2 After CISA processed and made productions of the documents located pursuant to its search, CISA located one additional document while finalizing the *Vaughn* index. This additional document is a slightly updated version of a document withheld in full pursuant to Exemptions (b)(5) and (b)(7)(E) (document number NPPD 000967). The 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.
their ideas, strategies, and advice in written communications. Department operations would be hampered because the disclosure of such preliminary assessments and opinions would make employees contributing to pre-decisional deliberations much more circumspect in providing their written views. This lack of candor will seriously impair the Department’s ability to foster the forthright internal discussions necessary for efficient and proper decision-making. Agency decision-making is best enhanced when employees are able to freely discuss and debate their views and are not tempered by considerations of public release of their discussions and internal pre-decisional deliberations.

17. Executive Branch staff prepare documents to brief, or to prepare to brief, senior leadership officials on pending questions on various legal and policy points. These documents are prepared in advance of an agency decision on these matters, and are for the purpose of informing, advising, deliberating, and/or recommending that the decisionmaker take (or not to take) a certain course of action. Such briefing materials are therefore pre-decisional, inasmuch as they precede the decision being advised on, and do not embody final agency action. The drafters of these briefing materials attempt to succinctly summarize particular events, identify important issues and questions, provide key background information, and may provide a recommendation — all in order to facilitate an official’s decision on the matter. Throughout this process, the drafters necessarily review and analyze the underlying circumstances and potential issues arising on the topic at hand, and then selectively craft materials to reflect the information and/or guidance that, in their judgment, is necessary and integral to aiding the decisionmaker’s determination on the question at hand. The documents reflect the drafters’ preliminary view of the facts and their relevancy. The decision to include or exclude certain information in or from analytical documents is therefore itself an important part of the deliberative process. The
agency’s senior officials rely heavily on the creation of such briefing materials so that they can
guide and/or make a determination on the substance of the many legal and policy issues being
considered by the agency every day in individual offices. CISA’s senior leaders are responsible
for carrying out CISA’s mission, which includes identifying and addressing the most significant
risks to critical infrastructure. The deliberative documents were provided to brief CISA’s senior
official aid those officials in making decisions regarding the assessment and management of
risks to critical infrastructure. Thus, disclosure of these documents would foreseeably harm the
decision-making process of the agency’s senior leadership by inhibiting the flow of staff-level
views and assessments.

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

19. **Contacts between the DHS and State election officials:** In the documents
concerning contacts between the DHS and State Election Officials, CISA withheld employees’
frank summaries of meetings with State election infrastructure officials that contained
recommendations, emphasized points, and key areas of concern. The documents further contain
staff assessments of the meetings and engagements with certain State officials and agency staff’s
then-current tracking and understanding of the status of vulnerabilities in certain States’ election
infrastructure, along with recommendations for future action as a result of those assessments and understanding. The assessments are not final and reflect substantial uncertainty. The documents were used only internally within DHS and were provided to agency leadership on an on-going basis to help leadership track the current status of staff engagement with State officials and to aid leadership in making decisions regarding prioritizing time and resources to meet emerging needs related to the agency’s election infrastructure security activities. Release of the documents would foreseeably harm the agency by inhibiting agency staff’s ability to communicate frank, current, non-final assessments to agency leadership, which would harm agency leadership decision-making by depriving them of developing information. Further, release of non-final information would give the public an erroneous understanding of the basis for agency decisions.

20. **Election Task Force Meeting Minutes:** In the Election Task Force meeting minutes documents, CISA withheld the deliberative information documented in the meeting minutes, which were shared only with the interagency partners on the Task Force. 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 contain 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 Task Force meeting minutes also reflect potential recommendations that the Task Force would make to agency leadership to inform planning, resourcing, and prioritization of DHS’s election infrastructure security efforts. Disclosure of the information would have a chilling effect on the deliberative discussions of meeting of agency task forces, which study particular issues and provide recommendations to
agency leadership. Chilling this communication between agency employees and between agency staff and leadership would foreseeably harm the agency by undermining the agency’s ability to perform its duties. CISA depends on the ability of its employees to offer candid ideas and opinions to agency decision-makers and to each other without the fear of public exposure; to curtail this process would be detrimental to CISA and all government entities.

21. **Election Infrastructure Cyber Risk Characterization Report:** CISA applied Exemption (b)(5) to protect pre-decisional deliberative information in a report concerning election infrastructure cyber risk characterization prepared by CISA’s Office of Cyber and Infrastructure Analysis for wider Departmental leadership consideration and to aid in decisions regarding areas where the agency could best help mitigate risk to election systems. The document was prepared for internal purposes only and contains select, non-final, in-process assessments and characterizations of election infrastructure vulnerabilities. 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 of the information would foreseeably harm the agency’s ability to assemble and communicate such information for leadership planning. Further, disclosing non-final assessments of vulnerabilities could mislead the public as to the reasons and basis for later agency actions and final assessment of facts.

22. **Incident Reports:** In the incident reports about vulnerabilities in election systems, CISA applied Exemption (b)(5) to protect non-final assessments of election infrastructure defense, agency staff analysis and recommendations, and coordination plans. The reports contain unverified, preliminary information, and timelines of on-going agency staff engagements
and discussions, which were documented for and provided to agency leadership for leadership’s
situational awareness and oversight to aid in planning of election infrastructure security efforts.
The reports also contained preliminary findings provided to another federal agency along with
recommended actions for that agency’s consideration. Disclosure of these reports would
foreseeably harm CISA’s ability to communicate clearly and frankly with other federal partners
and would harm CISA staff’s ability to provide transparent communication and assessments to
CISA leadership. Disclosure of non-final reports would also mislead the public by releasing
non-final assessments of sensitive information.

**Exemption 7(E)**

23. DHS withhold eight records pursuant to FOIA Exemption (b)(7)(E).\(^3\) Exemption
7(E) affords protection to all documents “compiled for law enforcement purposes” that “would
disclose techniques and procedures for law enforcement investigations or prosecutions, or would
disclose guidelines for law enforcement investigations or prosecutions if such disclosure could
reasonably be expected to risk circumvention of the law.”

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

---

\(^{3}\) Three documents related to contacts between the DHS and State Election Officials (NPPD 000419; NPPD 000944;
NPPD 000967); the Election Infrastructure Cyber Risk Characterization Report (NPPD 0000926 – 000942) and four
incident reports (NPPD 000962; NPPD 000963 – 000966; NPPD 001115 – 001119; NPPD 001095 – 001106). As
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.

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

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

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

---

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

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

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

29. Charts of contacts between NPPD and State Election Officials contain
information on the nonpublic techniques and procedures the agency uses to assess and address
risks to and vulnerabilities in States’ election infrastructure. For example, one chart contains
assessments of cyber hygiene vulnerabilities in States’ election infrastructure and NPPD’s
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.

6 See NPPD 000926–000942.
7 See NPPD 000963-000966.
8 See NPPD 000967.
Segregability

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

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

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

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

Dated the 15th day of May, 2020

__________________________________________
James V.M.L. Holzer
Deputy Chief FOIA Officer
DHS Privacy Office
U.S. Department of Homeland Security
<table>
<thead>
<tr>
<th>Bates Range</th>
<th>Page Number</th>
<th>Release Document Name</th>
<th>Description of Document</th>
<th>Date</th>
<th>Exemptions Applied</th>
<th>Explanation of Withholdings</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPPD 000351 - NPPD 000360</td>
<td>9-18</td>
<td>&quot;Weekly Summary for Meetings with Elections Infrastructure Officials&quot;</td>
<td></td>
<td></td>
<td>(b)(5) - deliberative process</td>
<td>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.</td>
</tr>
<tr>
<td>NPPD 000315 - NPPD 000360</td>
<td>2-4</td>
<td>&quot;Election Task Force Minutes&quot;</td>
<td>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.</td>
<td>Oct. 25, 2017</td>
<td>(b)(5) - deliberative process</td>
<td></td>
</tr>
<tr>
<td>NPPD 000505 - NPPD 000507</td>
<td>82-88</td>
<td>&quot;Election Task Force Minutes&quot;</td>
<td></td>
<td>Oct. 11 &amp; 12, 2017</td>
<td>(b)(5) - deliberative process</td>
<td></td>
</tr>
<tr>
<td>NPPD 000944</td>
<td>46</td>
<td>One spreadsheet describing engagement with 22 states by NPPD and one spreadsheet describing engagement with 3 states</td>
<td>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.</td>
<td></td>
<td>(b)(5) - deliberative process; (b)(7)(E)</td>
<td></td>
</tr>
<tr>
<td>NPPD 000967</td>
<td>63</td>
<td>Chart of the status of NPPD’s outreach to states regarding risk vulnerability and cyber hygiene assessments for states’ election infrastructure</td>
<td>Initially processed document undated</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NPPD Office of Cyber and Infrastructure Analysis record, documenting internal assessment of the election infrastructure and potential cyber vulnerabilities</td>
<td>Sept. 2016</td>
<td>(b)(5) - deliberative process; (b)(7)(E)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NPPD 000926 - NPPD 000942</td>
<td>64-80</td>
<td>Election Infrastructure Cyber Risk Characterization</td>
<td>NPPD Office of Cyber and Infrastructure Analysis record, documenting internal assessment of the election infrastructure and potential cyber vulnerabilities</td>
<td>CISA applied FOIA exemption (b)(7)(E) to protect 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NPPD 000926 - NPPD 000942</td>
<td>64</td>
<td>&quot;Election Infrastructure Cyber Risk Characterization&quot;</td>
<td>NPPD Office of Cyber and Infrastructure Analysis record, documenting internal assessment of the election infrastructure and potential cyber vulnerabilities</td>
<td>Sept. 2016</td>
<td>(b)(5) - deliberative process; (b)(7)(E)</td>
<td></td>
</tr>
</tbody>
</table>

Incident Reports about Vulnerabilities in Election Systems
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

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 also misleadingly provide non-final assessment information.

CISA applied FOIA exemption (b)(7)(E) to protect nonpublic reports of tests of state election infrastructure and vulnerability assessments. The reports were 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.

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.

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.
<table>
<thead>
<tr>
<th>Title</th>
<th>Timeline (July 28, 2016 through August 31, 2016) of emails/incident reports received by NPPD/NCCIC and responses pertaining to election security.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>July 28 - Aug. 31, 2016</td>
</tr>
<tr>
<td>Exemptions</td>
<td>(b)(5) - deliberative process; (b)(7)(E)</td>
</tr>
</tbody>
</table>

**Timeline (July 28, 2016 through August 31, 2016) of emails/incident reports received by NPPD/NCCIC and responses pertaining to election security.**

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.

**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.

**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.**

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.