DS Report on Security Incidents Related to Potentially Classified Emails sent to Former Secretary of State Clinton's Private Email Server

DS Office of Information Security,
Program Applications Division
DS/IS/APD

US Department of State

September 13, 2019

PURPOSE

This report was prepared by the Program Applications Division (DS/IS/APD, APD) of the DS Office of Information Security (DS/SI/IS), Bureau of Diplomatic Security (DS) in order to document the process by which several thousand potentially classified emails sent through former Secretary of State Hillary R. Clinton's private, non-US government email server were assessed to determine if any represented security incidents in accordance with the Department of State's (DoS) Security Incident Program as published in 12 FAM 550. While it is not typical for APD to document security incident investigations or groups of related security incident investigations in a comprehensive report, the exceptional nature of this event and high level of interest in its outcome justifies its production.

Attachment:
DS/IS/APD Administrative Timeline

I. BACKGROUND

In December 2014, representatives of former Secretary of State Hillary R. Clinton provided the Department of State with roughly 33,000 individual emails (the HRC emails) that were sent to or from her private email server during her tenure as Secretary of State. By May of 2015, an ongoing Freedom of Information Act (FOIA) review had determined that information in certain emails was classified at the time of the FOIA release. The FOIA review further raised questions as to whether there was information that should have been or was classified at the time the emails were sent.

In March of 2016, following significant discussion with DS, the Federal Bureau of Investigation (FBI) directed DoS to hold in abeyance any administrative actions relative to the potential mishandling of classified information. In July of that year, the FBI notified DoS that it had completed its investigation and the APD administrative effort resumed.

Over the next thirty-eight months, APD staff members reviewed thousands of pages of documents, received hundreds of individual statements, and met in-person with dozens of past and present DoS employees and senior officials. The APD focus was to determine two things: (1) if any of the emails under review represented a failure to properly safeguard classified information, and (2) if, in the instance of such a failure, any individual(s) could be determined to bear individual culpability.

II. PROCESS

The purpose of the Department's Security Incident Program is to enhance the protection of classified information by identifying, evaluating, and assigning responsibility for breaches of security. The program implements requirements found in Executive Order 13526, *Classified National Security Information* (E.O. 13526) and its implementation is regularly reported on to the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA), the oversight entity for E.O. 13526. The DoS definition of a security incident found in 12 FAM 550 reflects the framework set forth in E.O. 13526. Incidents are categorized as either violations or infractions based on the likelihood of unauthorized disclosure. An incident is categorized as a violation when it is "a knowing, willful, or negligent action that could reasonably be expected to result in the unauthorized disclosure of classified information." An incident is categorized as an infraction when it represents a failure to safeguard classified information but could not reasonably be expected to result in an unauthorized disclosure of classified information. Any introduction of classified material to an unclassified information system or network that results in its transmission outside DoS control is categorized as a violation.

The Program Applications Division (DS/IS/APD) within DS is responsible for administering the DoS Security Incident Program. That program is not primarily punitive, but rather its purpose is to enhance the protection of classified information by identifying, evaluating, and assigning responsibility for breaches of security. Additionally, APD provides individuals employed by the Department with remedial instruction and suggests process or policy changes when appropriate.

As such, the program helps ensure that information is properly safeguarded and that responsible individuals learn from their errors so that they can adapt their conduct in the future.

When a potential failure to properly safeguard classified information is identified, APD conducts an investigation in an attempt to establish two things: (1) whether a valid incident actually occurred (validity), and (2) whether individual culpability can be established for the incident (culpability).

In establishing validity, APD must determine that the reported condition actually represents a *"failure to safeguard classified"* information. This often involves a review to determine if a particular document or email was actually classified at the time of transmission. APD relies on extensive internal experience, input from the sender, and consultation with relevant subject matter experts to make this determination. If it is determined that the event does not represent a valid incident, either because the reported condition does not represent a failure to safeguard, or because it cannot be established that the information in question was classified at the time of the potential incident, it is dismissed as unfounded.

If validity can be established, APD will then attempt to assess individual culpability. The facts of the case as understood by APD will be presented to any individual suspected of bearing individual culpability so that they are made clearly aware of the ongoing administrative investigation and its potential outcomes, and are afforded an opportunity to provide a statement that they would like considered prior to adjudication. If the statement or circumstances mitigate individual culpability but do not invalidate the incident, it is adjudicated as "valid, but not culpable (VnC)".

If validity and culpability are both clearly established, the incident is simply adjudicated as valid and the individual is notified of the outcome. The individual is afforded a period of ten days in which to submit a written appeal of the adjudicative decision to the Director, DS/SI/IS. Reconsideration to the initial adjudication and any new information provided is reviewed. The Director may affirm the adjudication, downgrade a violation to an infraction, dismiss culpability, or invalidate the incident. The individual is notified in writing of the appellate decision. There is no further appeal of the adjudication.

In the case of DoS employees, valid violations are referred to the Conduct, Suitability, and Discipline Division of the Bureau of Human Resources (HR/ER/CSD) and to DS's Office of Personnel Security and Suitability (DS/SI/PSS). If the individual is a former Department of State employee, the violation is referred to DS/SI/PSS only. While every violation is referred, individual infractions are not, but accrued infractions over time will trigger referral if the infraction represents a third or subsequent incident in a 36-month period.

III. METHODOLOGY

The review of information referred to APD presented unique challenges in terms of volume, timing, complexity, and other factors described below. The Department followed the process set forth in 12 FAM 550, but needed to deploy certain methodologies to address duplicative email documents and other factors to complete the administrative review within a reasonable period of

time without compromising the integrity of the program or the privacy of the individuals involved.

Initially, in the summer and fall of 2016, APD was provided with hard-copy documentation of each email assessed by the DS Assistant Secretary, on advice of a DS classification review panel (DSCRP) to have been classified at the time of sending.

Within the thousands of individual email documents, APD often found duplication or later additions to individual email conversations. Sometimes these were linear conversations and sometimes they diverged and branched. APD's first effort was to collate these and group them into distinct email conversations.

Once the individual documents were sorted into conversations, and best exemplars of duplicative documentation were identified, APD reviewed each message thread to determine which individuals introduced classified information into that conversation and which merely passed the information along. This review process began in earnest in July 2016, and was briefly interrupted in October, at the request of the FBI, before resuming and concluding in late December 2016.

The initial approach to the categorization of potential incidents was that the individual responsible for the introduction of classified information to the network, which was then transmitted outside of DoS control, would be assessed a potential violation, while individuals who simply forwarded that information on would be assessed potential infractions. This provisional approach for assessing infractions was abandoned early in the process, however, as it very quickly became clear that it would be impossible to determine when an individual could reasonably be expected to know that content already on the system should have been classified by the originator. By the end of the process, APD was focused solely on the assessment of potential violations for individuals who introduced content which was assessed to have been classified at the time it was sent.

Once the documentation was sorted, APD began to review the potential incidents by focusing first on those individuals who communicated most regularly with former Secretary Clinton, then on other individuals who were still DoS employees, and finally on individuals who were no longer DoS employees. These reviews were completed in July 2018.

In April and May of 2019, the DS Front Office provided to APD the remaining emails that it assessed to contain classified information. Though the overall volume of these additional documents was much greater than the initial group from 2016, lessons learned throughout the process led to significant efficiencies in reviewing this second tranche of documents. APD reviewed and sorted these documents from May 5, 2019 until July 20, 2019, and began contacting individuals on July 22, 2019 to afford them the opportunity to provide a statement in accordance with Department regulations. The entire effort was completed on September 6, 2019, thereby concluding the investigative and adjudicative effort in this matter.

In the case of individuals who were either unreachable or otherwise non-responsive, DS implemented a slight modification to the appeals process. As noted above, an individual typically has ten days to contact the Director of the Office of Information Security to appeal an

adjudicative decision. In cases where the individual was no longer employed by the Department and could not be reached or was entirely unresponsive, the letter of notification of the adjudication was placed in that individual's security file in APD and their investigative file in DS/SI/PSS. The letter included a notation that the individual may appeal the decision whenever they become aware of it. This allows APD to conclude the administrative process while still protecting the individual's right to appeal should the matter come to their attention at some future date.

IV. CHALLENGES

The unprecedented nature and scale of this event posed many significant challenges to the APD staff's accomplishment of this effort. Specifically:

Scale

First, and perhaps most obvious, is the sheer scale of the effort. A typical spillage event involves a single email, not thousands of hard-copy documents to be sifted through. The scale alone caused considerable delay to the effort.

Information not marked as classified

A typical security violation involves pre-marked classified information discovered contemporaneously with the incident. None of the emails at issue in this review were marked as classified.

Severe Break in Time between Incident and Investigation

The significant break in time (five to nine years) between when the incidents occurred and when they were reviewed posed several serious challenges.

Typically, APD has access to the relevant individuals fairly contemporaneous to the incident itself. This makes it easier to schedule interviews and when individuals provide statements, the underlying events are still fresh in their memories. Additionally, relevant subject matter experts are readily available to assist in making an accurate determination of classification.

The break in time had the additional effect of making many of the individuals unavailable to be interviewed at all, as they have moved on from the Department and could not be reached.

The DoS Security Incident Program is designed to identify problem behavior and correct it. It is not inherently punitive. There is a natural progression to accountability and discipline when there is either recalcitrance or an egregious disregard for established practices. This event did not allow for this progression. Individual instances of problematic behavior that, if reported as they occurred, would be addressed in succession, were instead all addressed at one time so the individual did not have the benefit of an initial incident adjudication to modify his or her behavior to avoid subsequent incidents involving the same underlying behavior.

Individual Perception at Time of Sending and Original Classification Authority

In a spillage event that involves the transmission of classified information that was not clearly marked as classified, the perception of the sender at the time of sending becomes very important. In this case, APD did not have contemporary access to additional supporting information, and the assessment of classification was made years after the fact. This made establishment of culpability extremely difficult.

APD also does not typically adjudicate active classification determinations made by an original classification authority (OCA). If an individual held OCA at the time the message was sent and declares that they made an active determination that the information was not classified at the time, it is generally not feasible or appropriate to assign them culpability. An OCA cannot, however, ignore a classification determination if the information has already been classified by someone else, and they are aware of that existing determination. On the other hand, an OCA is not assumed to be aware of instances where similar information has been previously classified by another OCA but not documented.

Similarly, with respect to Foreign Government Information, which is defined in E.O. 13526 to be "information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence," the ultimate determination of classification turns on whether the foreign government provided information with the expectation of confidentiality. In these instances, the U.S. government interlocutor with the foreign government is ultimately best placed to assess whether and how the foreign government intended that certain information was to be held in confidence. Accordingly, the adjudications relied significantly on the perspectives of the individuals who held the communications with the foreign government.

V. ADJUDICATIVE RESULTS (TOP LINE ROLLUP)

APD's administrative review of the HRC emails resulted in the adjudication of 91 valid violations attributable to 38 individuals. Additionally, APD adjudicated 497 valid violations where no individual was found to bear culpability, resulting in a "valid, but not culpable" determination.

Total Valid Violations Adjudicated: 91
Total VnC: 497

VI. CONCLUSIONS / OBSERVATIONS

The APD effort to evaluate potentially classified emails sent to former Secretary Clinton's private email server in the context of the DoS security incident program involved thousands of person-hours of review and investigative effort, including gathering statements from hundreds of past and present DoS employees, and conducting dozens of interviews. Beyond assessing

individual incidents consistent with 12 FAM 550, APD also sought to determine if these incidents were representative of a larger pattern of classified information mishandling or a deliberate means to handle classified information outside of official channels. Careful consideration of the broader context has yielded the following observations and conclusions:

The Use of Personal Email to conduct Official Business Represented an Increased Risk of Unauthorized Disclosure

It was APD's determination that the use of a private email system to conduct official business added an increased degree of risk of compromise as a private system lacks the network monitoring and intrusion detection capabilities of State Department networks. While the use of a private email system itself did not necessarily increase the likelihood of classified information being transmitted on unclassified systems, those incidents which then resulted in the presence of classified information upon it carried an increased risk of compromise or inadvertent disclosure.

APD Uncovered No Persuasive Evidence of Systemic Misuse Relative to the Deliberate Introduction of Classified Information to Unclassified Systems

While there were some instances of classified information being inappropriately introduced into an unclassified system in furtherance of expedience, by and large, the individuals interviewed were aware of security policies and did their best to implement them in their operations. Correspondence with the Secretary is inherently sensitive, and is therefore open for broad interpretation as to classification, particularly with respect to Foreign Government Information. Instances of classified information being deliberately transmitted via unclassified email were the rare exception and resulted in adjudicated security violations. There was no persuasive evidence of systemic, deliberate mishandling of classified information.

Timeline
Department of State's Review of Classified Information on Former Secretary Clinton's Personal Server and Assessment of Potential Security Incidents

Dec 2014	Former Secretary Clinton provides the Department with roughly 30,000 emails from her personal server. Records appraisal efforts begin to determine which emails are federal records.
Apr – May 2015	Initial FOIA review determines that some of the emails contain classified and classifiable information per Executive Order 13526 on Classified National Security Information.
May 22, 2015	First FOIA release of a portion of Secretary Clinton's roughly 30,000 emails on the public FOIA website (https://foia.state.gov/Search/Collections.aspx).
May 27, 2015	State received court order to produce all emails by January 2016.
Feb 8, 2016	State/DS requests guidance from FBI regarding when normal administrative actions relative to potential mishandling of classified information may commence.
Feb 29, 2016	FOIA review of approximately 30,000 emails completed; Department makes online posting.
Mar 8, 2016	FBI directs State to hold in abeyance any administrative actions until further notice.
Jul 5, 2016	FBI announces completion of investigation.
Jul 17, 2016	DS/IS/APD resumes administrative review and assessment of potential security incidents.
July-August 2016	FBI provides State tens of thousands of documents from its investigation; State begins its records appraisal of this content.
October 7, 2016	State commences FOIA production of documents provided by FBI, posting online any releasable content.
Dec 16, 2016	The Department completes its initial assessment of first group of emails and prepares to begin investigative and adjudicative effort.
Jun 15, 2017	FBI provides State an additional 6,861 emails from an unrelated investigation which possibly contained emails to/from Former Secretary Clinton's private email address that had not yet been reviewed.
Dec 29, 2017	FOIA review of emails provided by the FBI in June 2017 completed.
July 23, 2018	Initial DS security incident review effort concluded pending receipt of additional documentation
Sep 28, 2018	FOIA review of all emails provided to State by FBI in July and August 2016 related to this matter is completed.
Apr-May, 2019	DS/IS/APD takes custody of second group of emails
May 10, 2019	DS/IS/APD begins administrative review of second group of emails
July 22, 2019	DS/IS/APD begins concurrent notification of all individuals identified as transmitting classified information in second group of emails
Sep 6, 2019	DS/IS/APD concluded investigative and adjudicative effort relative to the emails referred for security adjudication