United States Department of State

Washington, D.C. 20520

MAY 23 2017

The Honorable
Charles Grassley, Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Thank you for your March 30, 2017 letter regarding security clearances for certain former Department of State officials. The Department takes the security of its people, operations, and information very seriously.

Attached please find background information and responses to your questions. We hope the background information will provide some context so that our responses will be of maximum use to you.

Please let us know if we can provide the Committee with additional information about the Department's Security Incident Program or other security procedures.

Sincerely,

Joseph E. Macmanus
Bureau of Legislative Affairs

cc: The Honorable Dianne Feinstein

~~SENSITIVE BUT UNCLASSIFIED~~

Department of State Response to Chairman Grassley's March 30, 2017 letter

(U) *Overview of the Department's Security Practice and Procedures*

(U) The development and protection of sensitive and classified information is at the core of the Department's mission. Every day, thousands of Department personnel conduct their national security mission with care and discretion, including how they handle classified information. Each of them individually reflects the Department's collective commitment to protecting sensitive and classified information from unauthorized disclosure.

(U) The Department takes steps to ensure that information is properly stored and secured. In the event that Department personnel believe information was improperly handled, we have a well-established Security Incident Program for evaluating incidents, run by the Bureau of Diplomatic Security (DS). That process is outlined in our Foreign Affairs Manual, as well as in detail below.

(U) *The Department's Unique National Security Mission*

(U) Diplomatic information is often received and generated through open channels. For example, our diplomats speak to their foreign counterparts over unclassified phone lines and in public spaces. The Department also gathers significant information from public sources, such as foreign media reporting. At the same time, other U.S. agencies may develop the same or similar information through intelligence channels. As a result of this "parallel reporting," it is common and expected that the same information may be properly classified at different levels based on who collected it and how they collected it.

(U) Another example of how our unique national security mission manifests is through foreign government information (FGI), which is defined, *inter alia*, as "information provided to the United States Government by a foreign government…with the expectation that the information, the source of the information, or both, are to be held in confidence."[1] Although the unauthorized release of FGI is presumed to cause harm to the national security[2] – thereby qualifying as eligible to be Confidential classified information[3] – Department officials routinely receive such information through unclassified channels out of necessity. As noted above, diplomats engage in meetings with counterparts in open settings, have phone calls with foreign contacts over unclassified, open lines, and email with and about foreign counterparts via unclassified systems.

(U) Diplomats could not conduct diplomacy if doing so violated the law. Accordingly, both Executive Order 13526 and the Foreign Affairs Manual acknowledge that FGI can be maintained on systems that would otherwise be inappropriate for safeguarding information classified Confidential, so long as it receives a degree of protection at least equivalent to that required by the foreign government.[4] Consequently, maintaining FGI on unclassified systems

---

[1] Executive Order 13526 § 6.1(s).
[2] Executive Order 13526 § 1.1(d).
[3] Executive Order 13526 § 1.2(a)(3).
[4] Executive Order 13526 § 1.6 (e); 5 FAM 482.6d.

often does not amount to mishandling the information. When FGI is subject to public release under the Freedom of Information Act, the Department must take steps to formally classify it and redact it appropriately. When the Department does so, this formal classification to protect the FGI from public release can be misinterpreted to suggest that the information had been improperly stored on an unclassified system. That is not necessarily the case; it is a reflection of the system outlined above interacting with the Department's FOIA obligations. In fact, for certain agencies, Congress has specifically exempted FGI from public disclosure in FOIA regardless of its classification status, and such information may be withheld without classifying it under FOIA.[5] The Department is not among those agencies with an exemption, although it has pursued one for a number of years. Lacking such an exemption, the Department must classify FGI to protect it from public release under FOIA.

(U) *The Department's Security Incident Program*

(U) 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.[6]

(U) Overwhelmingly, Department personnel meet that high standard of performance. Through our Security Incident Program, the Department reviews the conduct of our personnel, as well as personnel from other agencies who serve in our facilities, to identify instances where they fall short.

(U) The Program Applications Division (DS/IS/APD) within DS is responsible for administering the identification, investigation, and adjudication portion of the Department's Security Incident Program. That program is not punitive. Its purpose is to identify instances of the mishandling of classified information and to identify those responsible. It helps ensure that information is properly protected and that responsible individuals learn from their errors so that they can adapt their conduct in the future. It is critical to understand the remedial and educational purpose of this program.

(U) In most cases, a security incident is identified through a facility inspection relating to the improper storage of physical documents or electronic storage devices. At overseas U.S. diplomatic facilities where Marine Security Guards (MSGs) are present, nightly inspections are conducted in areas designated for the processing and storage of classified information. Domestically, Uniformed Protection Officers (UPOs) conduct random inspections in the Department's main building and selected annexes. While traveling, the Secretary's classified travel policy incorporates safeguards for the protection of classified information, to include MSG and UPO coverage. Due to the MSG and UPO inspections, the Department has a much more aggressive and rigorous program of internal security inspections than most federal agencies.

(U) If someone (usually an MSG or UPO) finds classified information unsecured, he or she secures the information and submits a security incident notice to the appropriate security

---

[5] 10 U.S.C. § 130c(c).
[6] 12 FAM 551.

officer, who promptly investigates the incident. The results of that investigation are forwarded to DS/IS/APD, which adjudicates all security incidents. If an individual is identified as responsible for the incident, he or she has an opportunity to submit a statement on his or her behalf using the OF-118, the Record of Incident Form. The DS/IS/APD adjudicator examines the totality of the available information and determines whether i) the incident is unfounded, ii) the incident is valid but the individual is not culpable, or iii) the incident is valid and the individual is culpable. Valid security incidents may be categorized as "security infractions" or "security violations," based on whether there is a reasonable expectation that an unauthorized disclosure has occurred. A security infraction is an incident judged as not reasonably expected to result in an unauthorized disclosure of classified information, while a security violation is an incident judged as reasonably expected to result in an unauthorized disclosure.[7]

(U) DS/IS/APD subsequently sends a letter of notification to the individual advising him or her of the adjudication. If DS/IS/APD determines the incident is valid and the individual culpable, the letter of notification advises the individual of his or her right to appeal. Such an appeal is directed to the Office Director of the Information Security Division (DS/SI/IS). The DS/SI/IS Office Director considers the adjudication of the information and any additional information provided by the employee. The DS/SI/IS Office Director then renders a decision affirming the incident, downgrading a violation to an infraction, determining lack of culpability, or invalidating the incident. Subsequently, the DS/SI/IS Office Director provides a letter to the employee informing him or her of the appeal decision. There is no further appeal.

(U) When a security violation is adjudicated as valid and a Department of State employee is culpable, it is 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 who still has a clearance through the Department, the violation is referred to DS/SI/PSS only. Individual "infractions" are not referred; the threshold for referral of security infractions for disciplinary action and/or security clearance review is met when an employee receives a third infraction in a 36-month period. At that time, DS/IS/APD refers all three infractions to HR/ER/CSD and DS/SI/PSS.

(SBU) [redacted]

(SBU) [redacted]

[7] The current definition is based on E.O. 13526. Its predecessor order, E.O. 13292, defined violations as incidents where conditions existed that merely favored the *possibility* of a compromise. This change allows the Security Incident Program to provide a more flexible and accurate reflection of actual conditions. The Department implemented the changed definition in 2014.

(SBU) [redacted]

(~~SBU~~) *Security Clearance Actions*

(U) DS/SI/PSS is responsible for developing, implementing, and overseeing the Department's policy on personnel security investigations and adjudications. Information from DS/IS/APD's Security Incident Program is reviewed under the U.S. Government's Adjudicative Guidelines for Determining Eligibility for Access to Classified Information ("Adjudicative Guidelines"). Following a security violation, DS/SI/PSS may take action in connection with an individual's security clearance if the circumstances warrant it. This is a fact- and individual-specific process: the adjudication of a security clearance must take into account a careful assessment of the whole person, following the review of available, reliable information about the person, past and present, favorable and unfavorable.[8]

(~~SBU~~) In addition to receiving referrals from DS/IS/APD's Security Incident Program, DS/SI/PSS receives potentially derogatory information on employees from a number of other sources, including information developed through background investigations. The Department does not maintain data about adverse actions taken against security clearances attributable to specific referrals of security incidents. Instead, the Department records actions based on the security concerns presented under the Adjudicative Guidelines. Two guidelines – Guideline K (Handling Protected Information) and Guideline M (Use of Information Technology Systems) – are most closely aligned with the security concerns presented by information "security infractions" and "security violations."[9]

(~~SBU~~) All actions taken by PSS in response to information provided by DS/IS/APD's Security Incident Program, or any other source noted above, will be documented and permanently archived in the individual's security file. Security files are reviewed by DS/IS/PSS for periodic security clearance investigations or special investigations that occur when circumstances arise that in the Department's view may affect security clearance eligibility. The Department of State may also release a security file to another government agency for the following reasons: to make a determination of general suitability for employment or retention in employment, to grant a contract or issue a license, grant, or security clearance, pursuant to statutory intelligence responsibilities or other lawful purposes and pursuant to oversight review authority with regard to an agency's investigative responsibilities.

---

[8] *See* Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, which can be found online.

[9] Each of the violations or infractions would also present security concerns under Guideline E (Personal Conduct), but the scope of Guideline E is much broader than security incidents.

(U) With this background, the following are the answers, as of the date of this letter, to your questions. As requested in your letter, we have broken out each question and answer separately:

1. (U) "Does the State Department agree with the FBI's finding that Secretary Clinton and her staff were "extremely careless in their handling of very sensitive, highly classified information" and that "there is evidence of potential violations of the statutes regarding the handling of classified information .... "

(U) The quoted language in this question is from a statement that former FBI Director Comey gave at a press conference. To our knowledge it is not a finding of the FBI. The Department of State is not in a position to agree or disagree with former Director Comey's statement.

2. (U) "Does the State Department agree with the FBI's finding that "[t[here is evidence to support a conclusion that any reasonable person in Secretary Clinton's position, or in the position of those with whom she was corresponding about the matters, should have known that an unclassified system was no place for that conversation"?

(U) The quoted language in this question is from a statement that former FBI Director Comey gave at a press conference and to our knowledge, it is not a finding of the FBI. Department of State regulations (12 FAM 544.3(a)) state, "that normal day-to-day operations be conducted on an authorized automated information system (AIS), which has the proper level of security control to provide nonrepudiation, authentication and encryption, to ensure confidentiality, integrity, and availability of the resident information."

3. (U) "Does the State Department agree with the FBI's finding that despite not recommending criminal prosecution, "this is not to suggest that in similar circumstances, a person who engaged in this activity would face no consequences. To the contrary, those individuals are often subject to security or administrative sanctions."

(U) The quoted language in this question is from a statement that former FBI Director Comey gave at a press conference and to our knowledge, it is not a finding of the FBI. As set forth in the background introduction to this letter, the Department of State has extensive and long-standing processes related to the handling of classified information and the oversight of incidents of inappropriate handling. Each case is looked at individually and the incidences that Director Comey refers to are currently under review within the Department.

4. (U) "As a result of the FBI investigation, has the State Department begun a security review due to mishandling of classified information by Secretary Clinton and her colleagues and associates?" "If so, which individuals' clearances are part of the review?" "If not, why not?"

(~~SBU~~) The Department of State has a continuous and ongoing program for oversight of the handling of classified information. This program has operated for many years. The Department initiated a review of the handling of classified information in this matter as part of

that program, not as a result of the FBI investigation. The Department waited to begin its review until after the FBI concluded its investigation in order to avoid prejudicing the FBI investigation.

(~~SBU~~) All employees of the Department of State, or non-employees holding a State Department-issued security clearance, are subject to the security oversight programs of the Department. This would include any and all colleagues and associates of former Secretary Clinton who fall into those categories. The Department's review is ongoing. We do not discuss matters that are part of an open review.

5. (U) "As a result of the FBI investigation, has the State Department suspended or revoked Secretary Clinton's clearance or that of any of her colleagues or associates, to include her subordinates at State and her attorneys? If so, which individuals? If not, why not?"

(~~SBU~~) The Department's investigation is ongoing. We note that, as is the case for other former Secretaries of State, former Secretary Clinton retains access to materials "originated, reviewed, signed, or received" by her during her tenure as Secretary of State, both classified and unclassified, under the access provisions set forth in E.O. 13526, Sec. 4.4(a)(2).

(~~SBU~~) In addition, on page one of your letter, you state, "Recently, the State Department informed the Committee that six additional Secretary Clinton staff at State were designated as her research assistants..." Based upon your reference to "additional," we understand you to be asking about seven individuals designated for access to classified information under Section 4.4(a) of E.O. 13526. As of the date of this letter, those individuals retain access only to certain specified information and continue to be subject to Department of State security programs relating to the handling of classified information and subject to the Department's personnel security program. As noted in the answer to your question above, the Department's review is ongoing. We do not discuss matters that are part of an open review.

(U) We request that you protect the information in this response marked "SBU," for Sensitive But Unclassified as it is generally not appropriate for public release and contains law enforcement and personnel sensitive material. SBU is a State Department handling restriction prohibiting State Department personnel from sharing publicly information so marked. As a result, we note that the public release of any portion of the enclosed or information is not authorized by this communication and, should you wish to disclose any document or portions thereof, we ask that you provide the Department with a reasonable opportunity to inform the Committee of any sensitive information that should be safe-guarded.