

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

July 19, 2016

The Honorable Ashton Carter
Secretary
U.S. Department of Defense
1000 Defense Pentagon
Washington, D.C. 20301-1000

Dear Mr. Secretary:

As of October 1, 2015, the Office of the Director of National Intelligence calculated that 2,865,402 individuals are “in access” to Top Secret, Secret, and/or Confidential-level clearances, while a total of 4,249,053 are eligible to access classified information.¹ Of the more than 2.8 million individuals who are “in access” to classified information and hold security clearances, approximately 2.2 million, or about 80 percent, were sponsored by the Department of Defense.² These government and contractor employees are entrusted with a privilege to access classified information, and they are required to acknowledge and accept various responsibilities that accompany this privilege.

Under Executive Order 13526, security clearances are classified at one of three levels. These three levels correspond to the amount of potential damage to national security if the covered information is disclosed without authorization. Accordingly, the “Top Secret” classification applies to “information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave* damage to the national security.”³ The unauthorized disclosure of “Secret” information “reasonably could be expected to cause *serious* damage,” while the unauthorized disclosure of “Confidential” information “reasonably could be expected to cause damage to the national security.”⁴

The Code of Federal Regulations provides “Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.”⁵ The ultimate determination whether to grant or extend a security clearance, consistent with the interests of national security, is determined upon careful consideration of 13 guidelines.⁶ These guidelines include measurements of the

¹ OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER, 2015 ANNUAL REPORT ON SECURITY CLEARANCE DETERMINATIONS (2016) at 5, *available at* https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2015-Annual_Report_on_Security_Clearance_Determinations.pdf.

² PERFORMANCE ACCOUNTABILITY COUNCIL, CROSS AGENCY PRIORITY GOAL QUARTERLY PROGRESS UPDATE, INSIDER THREAT AND SECURITY CLEARANCE REFORM FY2016 QUARTER 1 at 27, *available at* <https://www.performance.gov/node/3407/view?view=public#progress-update>.

³ Exec. Order No. 13526 (Dec. 29, 2009). (emphasis added)

⁴ *Id.* (emphasis added)

⁵ 32 C.F.R. pt. 147 (2012).

⁶ *Id.*

security clearance applicant's: allegiance to the United States; susceptibility to foreign influence; preference for a foreign country over the United States; sexual behavior that may subject the individual to coercion, exploitation, or duress, or that reflects lack of judgment or discretion; questionable personal conduct; financial considerations; alcohol consumption; drug involvement; emotional, mental, and personality disorders; criminal conduct; security violations; outside activities that conflict with security responsibilities; and misuse of information technology systems.

While 11 of the 13 guidelines generally focus on an individual's social activities or personal viewpoints and health, two guidelines—K and M—specifically relate to whether the applicant has mishandled classified materials.

Adjudicative Guideline K—"Security violations"—states, in relevant part:

- (a) *The concern.* Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.
- (b) *Conditions that could raise a security concern and may be disqualifying include.*
 - (1) Unauthorized disclosure of classified information;
 - (2) Violations that are deliberate or multiple or due to negligence.⁷

Adjudicative Guideline M—"Misuse of Information technology systems"—states, in pertinent part:

- (a) *The concern.* Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.
- (b) *Conditions that could raise a security concern and may be disqualifying include:*
 - (1) Illegal or unauthorized entry into any information technology system;
 - (2) Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system;
 - (3) Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;
 - (4) Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.⁸

⁷ 32 C.F.R. §147.13 (2012).

Two specific criminal statutes set penalties for mishandling classified information. The felony statute, 18 U.S.C. § 793, carries a maximum sentence of ten years' confinement, while the misdemeanor statute,⁹ 18 U.S.C. §1924, carries a possible punishment of a fine and imprisonment of up to one year.¹⁰

In addition to prosecution for the mishandling of classified information, a security incident may result in an individual's denial of access to classified information, with a suspension, revocation, or termination of the individual's security clearance.¹¹

The possible penalties for mishandling classified materials are wide-ranging, from administrative penalties to ten years' confinement. To help the Committee understand the scope of Guideline K and M violations by Department of Defense employees and contractors, please produce the following documents and information as soon as possible, but no later than 5:00 p.m. on August 2, 2016:

1. Documents sufficient to show the number of cases opened under Guideline K for noncompliance with security regulations from January 1, 2009 through December 31, 2013. For all such cases, provide:
 - a. Documents sufficient to show the titles, General Schedules (GS) or military ranks, and the status as a government or contractor employee of the individuals who were suspected to violate Guideline K;
 - b. Documents sufficient to show whether each of the individuals faced no administrative action, suspension, revocation, or termination of their security clearance; and

⁸ 32 C.F.R. §147.15 (2012).

⁹ 18 U.S.C. §793 states, in pertinent part:

Gathering, transmitting or losing defense information:

(e) Whoever, lawfully having possession of, access to, control over, or being entrusted with any . . . information, relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any . . . information, relating to the national defense,

(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed . . .

Shall be fined under this title or imprisoned not more than ten years, or both.

¹⁰ 18 U.S.C. §1924 states, in pertinent part:

Unauthorized removal and retention of classified documents or material:

(a) Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

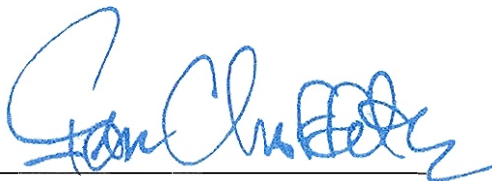
¹¹ Exec. Order No. 12968 Sec. 5.2 (Aug. 2, 1995).

- c. Documents sufficient to show whether each of the individuals were prosecuted under 18 U.S.C. §793 or 18 U.S.C. §1924.
2. Documents sufficient to show the number of cases opened under Guideline M for noncompliance with security regulations from January 1, 2009 through December 31, 2013. For all such cases, provide:
 - a. Documents sufficient to show the titles, General Schedules (GS) or military ranks, and the status as a government or contractor employee of the individuals who were suspected to violate Guideline M;
 - b. Documents sufficient to show whether each of the individuals faced no administrative action, suspension, revocation, or termination of their security clearance; and
 - c. Documents sufficient to show whether each of the individuals were prosecuted under 18 U.S.C. §793 or 18 U.S.C. §1924.

Please deliver your response to the Majority staff in room 2157 of the Rayburn House Office Building and the Minority staff in room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive your response in electronic format. An attachment contains additional instructions for responding to the Committee's request.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

Please contact Sang Yi with the Majority staff at (202) 225-5074 with any questions about this request. Thank you for your attention to this matter.



Jason Chaffetz
Chairman

Sincerely,



Ron DeSantis
Chairman
Subcommittee on National Security

Enclosure

cc: The Honorable Elijah E. Cummings, Ranking Member

The Honorable Stephen F. Lynch, Ranking Member
Subcommittee on National Security

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
 - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
 - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document;

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH,
PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE,
SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM,
CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE,
DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,
INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.
6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.
17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.

19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.
3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms “person” or “persons” mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term “referring or relating,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term “employee” means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.