United States Government Accountability Office

Report to the Honorable Christopher S. Murphy, U.S. Senate

April 2021

NATIONAL SECURITY

DOD and State Have Processes for Formal and Informal Challenges to the Classification of Information

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-294

GAO@100 Highlights

Highlights of GAO-21-294, a report to the Honorable Christopher S. Murphy, U.S. Senate

April 2021

NATIONAL SECURITY

DOD and State Have Processes for Formal and Informal Challenges to the Classification of Information

Why GAO Did This Study

Classified national security information is vital to U.S. national interests. The appropriate protection and handling of this information is a top priority for the executive branch and Congress. Based on guidance, such as Executive Order 13526, *Classified National Security Information*, authorized holders with access to classified information may submit a classification challenge if there are reasons to believe information is improperly classified. According to DOD and State officials, Members may also submit a classification challenge.

GAO was asked to review the processes for challenging the classification of national security information. This report describes (1) the processes to challenge the classification of information at DOD and State; and (2) the processes that Members of Congress can use to challenge the classification of information at DOD and State.

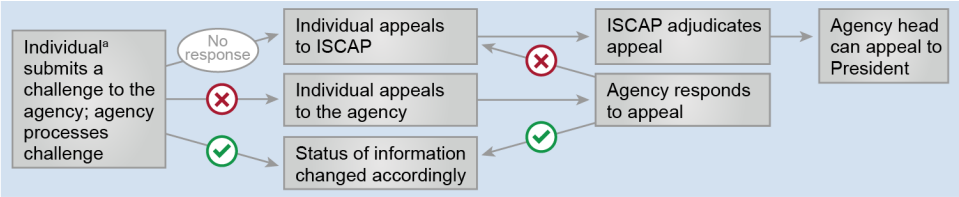
GAO reviewed applicable laws and regulations, and DOD, State, and other guidance related to the classification of information and classification challenge processes. GAO also interviewed DOD, State and ISOO officials.

View GAO-21-294. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or Kirschbaumj@gao.gov.

What GAO Found

The Department of Defense (DOD) and the Department of State (State) have similar processes for formal challenges to the classification of information. For example, if there is reason to believe that information is improperly classified, authorized holders—including executive branch agency or contractor personnel with relevant clearances—can submit a formal classification challenge in writing (see figure). Officials will then review the classification challenge and make a determination. If a formal challenge is denied, the authorized holder can then appeal to senior officials within the agency, and if the agency denies the appeal, the authorized holder can appeal directly to the Interagency Security Classification Appeals Panel (ISCAP). ISCAP, established by Executive Order, then issues a decision that is final unless the head of the agency appeals ISCAP's decision to the President.

Processes for Formal Challenges to the Classification of Information



Source: GAO analysis of Department of Defense, Department of State and Information Security Oversight Office information. | GAO-21-294

[a]Individual refers to an authorized holder with access to classified information.

Both DOD and State encourage authorized holders to resolve classification challenges informally before pursuing a formal classification challenge. According to DOD and State officials, informal challenges can be done in person, by phone, or by email. For example, officials told GAO that authorized holders can contact the relevant information security office about whether classified documents are marked properly.

According to DOD and State officials, Members of Congress (Members) may use their existing processes to formally and informally challenge the classification of information. However, according to officials from the Information Security Oversight Office (ISOO), which provides support to ISCAP, Members cannot appeal a decision to ISCAP. Instead, Members can appeal to the Public Interest Declassification Board (PIDB), a statutory body that makes recommendations to the President in response to certain congressional requests to evaluate the proper classification of records. DOD officials stated that they do not have any knowledge of ever receiving a formal classification challenge from Members. State officials stated that they did not receive any formal classification challenges from Members in 2017 through 2020. ISOO officials also stated that the panel received its first formal classification challenge from a Member in 2020. ISCAP subsequently denied the challenge and directed the Member to the PIDB.

Contents

Abbreviations

DOD	Department of Defense
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
Members	Members of Congress
NARA	National Archives and Records Administration
OCA	Original Classification Authority
PIDB	Public Interest Declassification Board
State	Department of State

441 G St. N.W.
Washington, DC 20548

April 16, 2021

The Honorable Christopher S. Murphy
United States Senate

Dear Senator Murphy:

Classified national security information is vital to U.S. national interests. The appropriate protection and handling of this information is a top priority for the executive branch, judiciary and Congress. In 2010, Congress passed and the President signed the Reducing Over-Classification Act, which required Inspectors General to conduct evaluations related to the proper classification of information in their respective agencies.[1]

The U.S. government classifies national security information as Confidential, Secret, or Top Secret if its unauthorized disclosure could damage the national security of the United States, among other conditions.[2] The U.S. government labels information as classified based on an original classification decision or derivative classification. Derivative classification is the incorporation, paraphrasing, restating or generation of information in new form that is already classified, and marking it

[1]Pub. L. No. 111-258, § 6(b) (2010). Section 6(b) of the Act required the inspector general of each department or agency with original classification authority to carry out two evaluations by September 30, 2016, related to classification and misclassification of information. Misclassification is not defined in the Act but, according to Department of Defense (DOD) officials, is generally understood as the act of classifying material at a higher or lower level of classification than would be appropriate under current standards for classifying information. The Act also authorized incentive programs for proper classification and required agency heads to establish training regarding the proper use of classification markings, among other topics. *See* §§ 6(a), 7 (codified at 50 U.S.C. § 3344).

[2]*See* Exec. Order No. 13,526, §§ 1.1, 1.2, 1.4 (Dec. 29, 2009). The Executive Order addresses the classification of national security information rather than information classified under the Atomic Energy Act of 1954. Our report similarly focuses on national security information. Under the Executive Order, information may be classified at one of three levels, defined by reference to the damage to national security that unauthorized disclosure could reasonably be expected to cause, as identified or described by the original classification authority. “Confidential” is applied to information for which unauthorized disclosure reasonably could be expected to cause damage; “Secret” is applied to information for which unauthorized disclosure reasonably could be expected to cause serious damage; and “Top Secret” is applied to information for which unauthorized disclosure reasonably could be expected to cause exceptionally grave damage. Exec. Order No. 13,526, § 1.2(a).

accordingly.[3] Original classification by an Original Classification Authority (OCA) typically results in the creation of a security classification guide, which is used by derivative classifiers and identifies what information should be protected through classification, at what level, and for how long.[4] Under Executive Order 13526, *Classified National Security Information*, and implementing regulations and agency guidance, authorized holders with access to classified information, which includes executive branch agency personnel and contractor personnel with relevant clearances, are encouraged and expected to challenge the classification status of information when they believe it is improper or should be unclassified.[5] According to Department of Defense (DOD) and Department of State (State) officials, Members of Congress (Members) may also submit a formal classification challenge.

The Information Security Oversight Office (ISOO)—a component of the National Archives and Records Administration (NARA)—in consultation with the National Security Advisor, is responsible for overseeing the federal government's Classified National Security Information program. Additionally, each executive branch agency that handles classified information, to include DOD and State, has an office that administers their information security program. For example, the Under Secretary of Defense for Intelligence and Security is the senior DOD official responsible for the direction, administration, and oversight of DOD's information security program. For State, the Bureau of Administration and Bureau of Diplomatic Security share responsibility for the implementation of State's information security program.

[3]Executive Order 13526 defines derivative classification as the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking it consistent with the classification markings that apply to the source information. It includes the classification of information based on classification guidance. Exec. Order No. 13,526, § 6.1(o).

[4]Executive Order 13526 defines original classification as an initial determination that information requires protection against unauthorized disclosure in the interest of the national security. Exec. Order No. 13,526, § 6.1(ff).

[5]The Executive Order defines an "authorized holder" of classified information as anyone who satisfies the conditions for access listed in section 4.1(a) of the order. That section states that a person may have access to classified information provided that (1) a favorable determination of eligibility has been made by an agency head or designee, (2) the person has signed an approved nondisclosure agreement, and (3) the person has a need-to-know the information. Exec. Order No. 13,526, §§ 6.1(c), 4.1(a).

You asked us to review the processes for challenging the classification of national security information.[6] This report describes: (1) the processes to challenge the classification of information at DOD and State; and (2) the processes that Members of Congress can use to challenge the classification of information at DOD and State.

The scope of this report focuses on the classification challenge processes at DOD and State because these organizations play a primary role in the classification of information and they conduct national security and foreign policy activities that tend to include classified information.

To address objective one, we reviewed applicable laws; DOD, State, and ISOO regulations; and other guidance related to the classification of information and the classification challenge processes. In addition, we interviewed DOD, State and ISOO officials about existing processes that are used to challenge the classification of information, including both formal and informal classification challenge processes. Finally, we reviewed the *2017 ISOO Report to the President* that included the latest available information on the number of formal classification challenges and their outcomes.[7] We assessed the reliability of these data by conducting interviews about data quality of the information contained in the report. We determined that the data were sufficiently reliable for our purposes of presenting the number of formal classification challenges reported across agencies.

To address objective two, we reviewed applicable laws; DOD, State, and ISOO regulations; and other guidance related to the classification challenge processes to determine if the guidance addresses classification challenges by Members. We also interviewed DOD, State, and ISOO officials about how Members use their respective processes to challenge the classification of information

We conducted this performance audit from March 2020 to April 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our

[6]This review was conducted in response to a 2020 request from Senator Christopher Murphy, then Ranking Member, Subcommittee on Legislative Branch, Senate Committee on Appropriations.

[7]National Archives and Records Administration (NARA), *2017 Information Security Oversight Office (ISOO) Report to the President* (May 2018).

findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Since the 1950s, a series of presidential executive orders have provided guidance to the Executive Branch regarding the classification, safeguarding, and declassification of national security information. The current order in effect is Executive Order 13526, *Classified National Security Information*.[8] ISOO is responsible for issuing directives to implement Executive Order 13526, overseeing agency activities to ensure compliance with the order and implementing directives, and annually reporting to the President on its implementation.[9]

Each executive branch agency that handles classified information is generally responsible for overseeing information security, including safeguarding classified national security information in its possession and issuing related guidance.[10] For example, DOD issued DOD Instruction 5200.01 and DOD Manual 5200.01, which provide guidance on classification, safeguarding, and declassification of national security information.[11] According to DOD officials, DOD is the largest generator of classified information in the federal government. Similarly, State issued

[8]Exec. Order No. 13,526, *Classified National Security Information*, 75 Fed. Reg. 707 (Dec. 29, 2009). Under the Executive Order, the authority to classify information originally may be exercised only by the President and Vice President; agency heads (including the heads of the military departments) and officials designated by the President; and U.S. government officials delegated this authority under the Order. *Id.* § 1.3.

[9]The Director of ISOO carries out these responsibilities under the direction of the Archivist of the United States and in consultation with the National Security Advisor. The Director of National Intelligence, after consultation with the heads of affected agencies and the Director of ISOO, may issue implementing directives with respect to the protection of intelligence sources, methods, and activities. *Id.* §§ 5.1, 5.2.

[10]Executive Order 13526 requires the heads of such agencies to designate a senior agency official to direct and administer the program established under the Executive Order, including promulgating implementing regulations, establishing education and training programs, and establishing and maintaining ongoing self-inspection programs. Exec. Order No. 13,526, § 5.4(d).

[11]DOD Instruction 5200.01, *DOD Information Security Program and Protection of Sensitive Compartmented Information (SCI)* (Apr. 21, 2016) (incorporating change 2, effective Oct. 1, 2020); DOD Manual 5200.01, vol. 1, *DOD Information Security Program: Overview, Classification, and Declassification* (Feb. 24, 2012) (incorporating change 2, July 28, 2020). DOD Manual 5200.01 includes two other volumes covering the marking of information and the protection of classified information.

guidance in the Foreign Affairs Manual to implement its classification processes.[12]

In addition, there are several processes implemented at executive branch agencies that may involve the declassification of national security information, such as the Mandatory Declassification Review process and the Freedom of Information Act process. The Mandatory Declassification Review process generally allows a member of the public to request a review of records containing specific classified information. According to ISOO officials, in practice, Mandatory Declassification Review processes have traditionally been associated with declassifying historical information, although that is not always the case. The Freedom of Information Act process also provides the public a process to request a broader set of records from a federal agency and, if this information contains classified national security information, an agency will assess whether it should remain classified.

Executive Order 13526 and implementing regulations in part 2001 of Title 32, *Code of Federal Regulations*, establish a means for authorized holders to challenge the classification of information, which we refer to in this report as a "classification challenge."[13] Further, the Executive Order and associated implementing regulations require agencies to establish procedures for challenges, and make the Interagency Security Classification Appeals Panel (ISCAP) responsible for hearing appeals from agency decisions on formal classification challenges.[14] Finally, the implementing regulations also note that informal inquiries from authorized

[12]Department of State, Foreign Affairs Manual (FAM), 5 FAM 480, *Classifying and Declassifying National Security Information—Executive Order 13526* (Oct. 31, 2018). State has also issued security information regulations in part 9 of Title 22 of the *Code of Federal Regulations*.

[13]The classification challenge process allows an authorized holder to submit a classification challenge if they believe in good faith that the information's classification status is improper and that it should be classified at a higher or lower level, or should be unclassified. *See* Exec. Order No. 13,526, § 1.8; 32 C.F.R. § 2001.14.

[14]The Interagency Security Classification Appeals Pane (ISCAP) is established under Executive Order 13526 for the purpose of advising and assisting the President, and is comprised of voting members from several agencies, including DOD and State. *See* Exec. Order No. 13,526, § 5.3(a), (e); 32 C.F.R. §§ 2003.6(b), 2003.4(a), 2003.1. The Director of ISOO serves as the ISCAP Executive Secretary, and ISOO staff provide program and administrative support.

holders should be encouraged to hold down the number of formal challenges and to ensure the integrity of the classification process.

In addition to these processes and entities, the Public Interest Declassification Board (PIDB) has a role in the declassification of information. Established and governed by statute, the PIDB generally advises the President and other executive branch officials on matters related to classification and declassification of information.[15] As discussed below, the PIDB may also review and make recommendations to the President in response to certain congressional requests to declassify or to evaluate the proper classification of records.

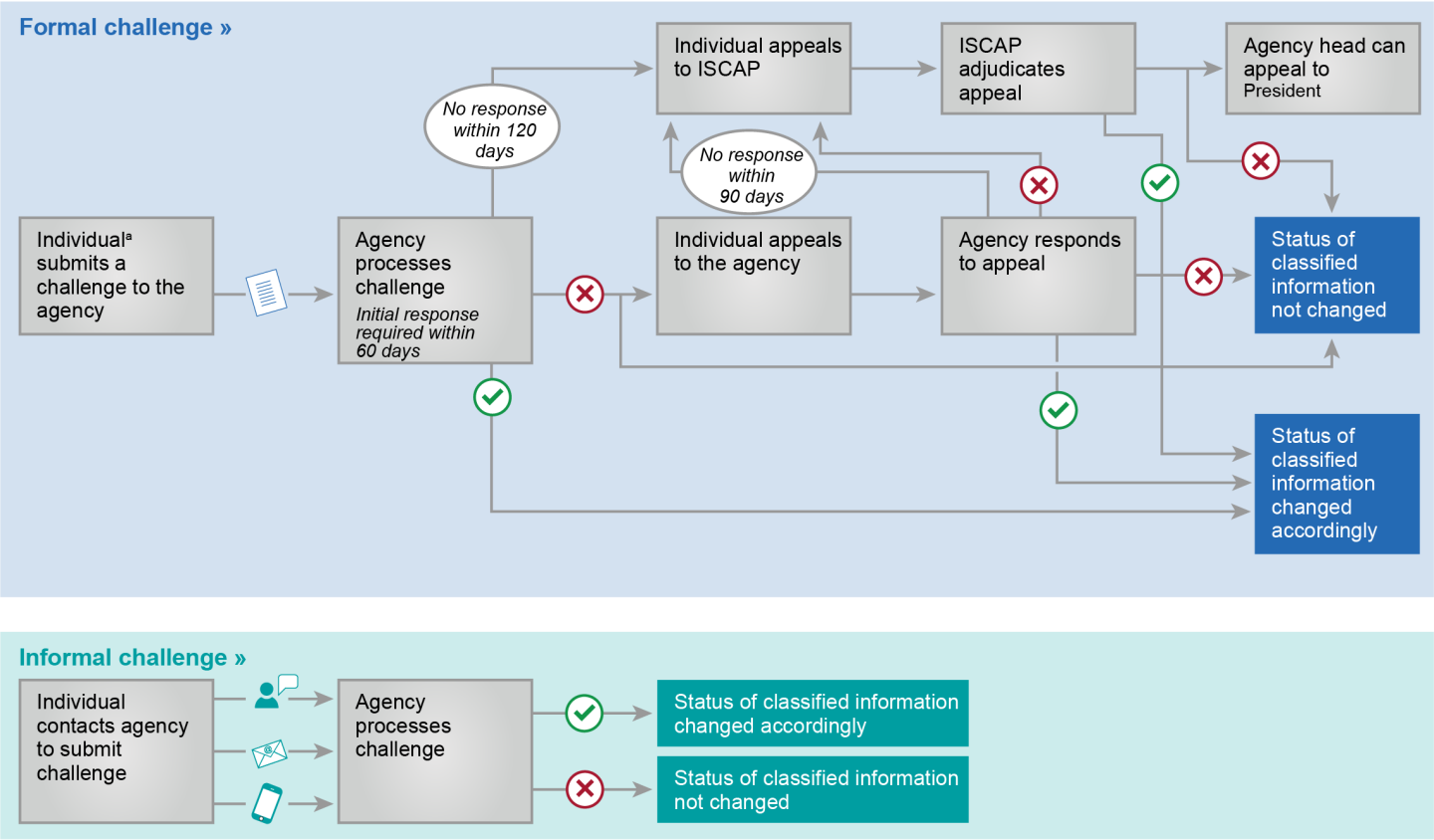
DOD and State Have Processes for Formal and Informal Challenges to the Classification of Information

DOD and State have processes for authorized holders to formally and informally challenge the classification of information, as shown in figure 1 below. The guidance issued by ISOO, DOD, and State encourage authorized holders (hereafter individuals) to resolve classification challenges informally before pursuing a formal classification challenge.[16] As a result, DOD and State officials noted that informal challenges are more common than formal challenges.

[15]50 U.S.C. § 3355a (a), (b). The PIDB is comprised of nine U.S. citizens preeminent in certain fields; the President appoints five of the members and the Speaker of the House, minority leader of the House of Representatives, and majority and minority leaders of the Senate each appoint one. Similar to the ISCAP, the Director of ISOO serves as the PIDB Executive Secretary, and ISOO staff may provide support. § 3355a(c), (d)(2), (j).

[16]*See* 32 C.F.R. § 2001.14(c); DOD Manual 5200.01, vol. 1, encl. 4, para. 22.a(1); 22 C.F.R. § 9.8(a). The ISOO regulations note that informal inquiries should be encouraged as a means of holding down the number of formal challenges and to ensure the integrity of the classification process. § 2001.14(c).

Figure 1: Processes for Formal and Informal Challenges to the Classification of Information at Executive Branch Agencies



ISCAP Interagency Security Classification Appeals Panel

Source: GAO analysis of Department of Defense, Department of State and Information Security Oversight Office information. | GAO-21-294

[a]Individual refers to an authorized holder with access to classified information.

Processes for formal challenges. DOD and State have similar processes for formal challenges to the classification of information. DOD and State's processes for formal challenges explain that authorized holders with access to classified information are encouraged to submit a classification challenge if there are reasons to believe the information is improperly classified or should be unclassified. According to ISOO, the executive branch reported 721 formal classification challenges in fiscal year 2017, of which DOD reported 677 and State reported that it did not

receive any.[17] If a formal challenge is denied, the individual must first appeal within the executive branch agency before appealing directly to ISCAP. The individual may also forward the challenge to ISCAP if the agency does not respond within specified timeframes.[18] An ISCAP decision about the appeal is final, unless the agency head chooses to appeal the decision to the President.[19] According to ISOO officials, since 2015, ISCAP received four classification challenge appeals and rendered decisions on all of them. According to ISOO officials, ISCAP administratively closed three out of four cases and overturned the agency's decision on the other case.

DOD. To initiate a formal classification challenge at DOD, an individual first submits a written description of the classification challenge to the department.[20] According to DOD officials, an example of a formal challenge includes a written request on official letterhead, in a memorandum with a signature, or requests by email. Second, DOD processes the challenge and submits the review of the classification challenge to the relevant OCA. DOD officials stated that the OCA will then consult the appropriate security classification guide and review the formal challenge to assess whether the information has been misclassified.

[17]Fiscal year 2017 is the most recent year that ISOO reported formal classification challenges. According to ISOO officials, in fiscal year 2017, none of DOD's formal classification challenges were sent to ISCAP for appeal. Since then, DOD officials stated that they relied more on informal classification challenges and had few, if any, formal classification challenges. While State reported that it did not receive any formal classification challenges in fiscal year 2017, State officials noted that they received one formal classification challenge in 2019. ISOO's report does not include further details, such as a breakdown of all the formal classification challenges by agency or the types of challenges by classification level.

[18]The agency must provide an initial written response within 60 days; if unable to respond within that time, it must acknowledge the challenge and provide a date by which it will respond. If no agency response is received within 120 days, the challenger may forward the challenge to ISCAP for a decision. Additionally, a challenger may forward a challenge to ISCAP if an agency has not responded to an internal agency appeal within 90 days. 32 C.F.R. § 2001.14(b)(3).

[19]The formal classification challenge procedures do not provide for an authorized holder to appeal an ISCAP decision to the President. According to ISOO officials, it is rare for an agency head to appeal decisions to the President.

[20]According to DOD officials, a formal classification challenge can be brought by any authorized holder with access to classified information. For example, an office within DOD could receive a formal classification challenge from an authorized holder from the same or a different office within DOD; a DOD contractor; or a different executive branch agency, such as State.

Third, based on the OCA decision, DOD is to provide a written response to the formal classification challenge within 60 days.[21] Fourth, the individual can either accept or appeal DOD's decision. If an individual appeals to DOD, the challenge will be reviewed by an impartial DOD official or panel. For example, the Department of Navy's guidance indicates that an impartial panel of OCAs would address appeals to formal classification challenges.[22] Finally, the individual can either accept DOD's final decision or further appeal a denial to ISCAP.[23] In addition, throughout the classification challenge process, there are several opportunities for the individual to appeal directly to ISCAP if the agency does not respond.[24]

DOD guidance encourages classification challenges and, DOD officials stated that in some cases, a formal challenge can change the information's classification level.[25] For example, DOD officials described a recent case where a formal classification challenge about military personnel overseas was forwarded to relevant OCAs in several offices, to include the Office of the Under Secretary of Defense for Policy, Office of the Under Secretary of Defense for Intelligence and Security, and Joint Staff. As a result of the formal classification challenge, the Office of the Under Secretary of Defense for Policy ultimately decided to declassify the information.

State. To initiate a formal classification challenge at State, an individual first submits a formal challenge in writing to an OCA with jurisdiction over the information or directly to the Bureau of Administration, Office of

[21]DOD components must provide an initial written response within 60 days and, if not responding fully to the challenge within that time, must acknowledge the challenge and provide an expected date of response. The acknowledgment must also advise the individual of their right to forward the challenge to ISCAP if no response is received within 120 days. DOD Manual 5200.01, vol. 1, encl. 4, para. 22.b(4).

[22]Secretary of the Navy Instruction 5510.36B, *Department of the Navy Information Security Program*, encl. 2, para. 2.f (July 12, 2019).

[23]The ISCAP procedures, found in section 2003.11 of Title 32, *Code of Federal Regulations*, do not specify a timeline for ISCAP's response to an appeal. According to ISCAP officials, ISCAP prioritizes appeals above other requests. However, because of the small staff size, there may be some delays in responding.

[24]If DOD does not respond to the formal classification challenge within 120 days, the individual may appeal directly to ISCAP. Similarly, if DOD does not respond to an agency appeal within 90 days, the individual may appeal directly to ISCAP.

[25]DOD Manual 5200.01, vol. 1, encl. 4, para. 22.b.

Information Programs and Services.[26] Second, according to State officials, State processes the challenge and the Bureau of Administration will forward the formal challenge to the relevant OCA. During this review process, officials will consult the security classification guide and review the formal challenge to assess whether the information has been misclassified. Third, based on the review, State is to provide a written response to the formal classification challenge within 60 days. Fourth, the individual can either accept or appeal State's decision. If an individual appeals a denial to State, the challenge will be reviewed by State's Appeals Review Panel. Finally, if the individual uses State's Appeals Review Panel to appeal the decision, the individual can either accept the decision or further appeal a denial to ISCAP. In addition, throughout the classification challenge process, there are several opportunities for the individual to appeal directly to ISCAP if State does not respond.[27]

As an example of this process, an individual may believe State information that is classified should not be classified. According to State officials, depending on the topic, State's Bureau of Administration would either reach out to the OCA responsible to discuss the level of classification or review whether other agencies have already publicly released the information as part of an existing Mandatory Declassification Review or Freedom of Information Act request. Officials stated that after the Bureau of Administration consults the appropriate security classification guide, and if the OCA agrees, the Bureau of Administration will revise the information's classification level and inform relevant parties of the change.

Processes for informal challenges. Both DOD and State have processes to question or challenge the classification of information informally. Officials described informal challenges as comparable to ongoing conversations and may take place in a variety of ways. For example, an individual may informally challenge the classification level of information in person, by phone, or email. Officials stated that while formal classification challenges are documented in writing and include an

[26]5 FAM 487; 22 C.F.R. § 9.8(a). If sent to the OCA, a copy is to be provided to the Office of Information Programs and Services.

[27]If State does not respond to the formal classification challenge within 120 days, the individual may appeal directly to ISCAP. Similarly, if State does not respond to an agency appeal within 90 days, the challenger may appeal directly to ISCAP.

appeal process, informal challenges generally lack documentation and appeal processes.

DOD. According to DOD officials, individuals can informally contact the OCA or the relevant information security office to question the classification of information. For example, according to DOD officials, an individual may informally question whether classified documents are marked properly.

State. State officials noted that individuals can informally contact the Bureau of Diplomatic Security's Office of Information Security by phone or in person to question the classification of information. According to State officials, the Bureau of Diplomatic Security then coordinates with bureaus to find the OCA responsible for the information. State officials stated that the Bureau of Administration's Office of Information Programs and Services can also be contacted informally with classification questions. For example, according to State officials, individuals have informally questioned whether State will release classified information at a lower classification level or at an unclassified level.

Members of Congress May Use Some Existing Processes to Formally and Informally Challenge the Classification of Information

Formal processes available to Members. DOD and State officials stated that Members of Congress could use the agency formal classification challenge processes described above, to challenge the classification of information. However, DOD officials stated that they do not have any knowledge of ever receiving a formal classification challenge from Members. State officials also told us that during their time in office, they did not receive any formal classification challenges from Members in 2017 through 2020. According to DOD and State officials, Members could initiate a formal classification challenge in writing. In addition, DOD and State officials explained that Members could have their formal classification challenge reviewed by an impartial DOD or State official or panel.

ISOO officials stated that ISCAP received its first and only formal classification challenge from a Member, specifically a Senator, in 2020. The Panel is responsible for hearing appeals of agency determinations. The Senator submitted a classification challenge to the National Security Council and, according to ISOO officials, the Senator appealed directly to ISCAP after the National Security Council did not respond to the challenge. In an August 2020 letter to the Senator about this challenge, the ISCAP Executive Secretary explained that he had determined that the appeal did not meet the requirements of Executive Order 13526 and, as a result, had administratively closed the case. The letter indicated that

Congress had provided itself with a unique and specific process by authorizing the PIDB to receive congressional requests to declassify or evaluate the proper classification of certain records. The August 2020 letter to the Senator further advised the Senator how he could initiate a review by the PIDB. According to ISOO officials that administratively support the PIDB, since 2014, the PIDB received three requests from Members, including one recently from the Senator who submitted the ISCAP challenge earlier in 2020.[28]

After the Senator's 2020 challenge, ISOO officials told us that appeal to ISCAP is not available to Members. ISOO explained the decision that the Senator's 2020 challenge did not meet the requirements of Executive Order 13526. They stated that the Executive Order provides for classification challenges by "authorized holders" of classified information and defines that term in a manner that would not include Members of Congress.[29] The officials noted that a Member of Congress does not receive a determination of eligibility by an agency head or a nondisclosure agreement for access, and stated that the term "authorized holder" as defined in the Executive Order would therefore not apply to Members for purposes of classification challenges to ISCAP. Accordingly, under a strict reading of the text, appeal to ISCAP would be unavailable.[30] By contrast, DOD officials stated that the department would consider Members to be "authorized holders," eligible to submit a formal classification challenge to DOD. DOD's comments on a draft of this report

[28]According to ISOO officials, PIDB declined one of the requests because of the large volume of records involved. In another request, the PIDB recommended to the President that the document, related to the war in Afghanistan, be declassified in part and a redacted version be released to the public. As of February 2021, PIDB has not yet made a final decision on the Senator's request.

[29]The ISCAP member body consists of senior level representatives appointed by the Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor. According to ISOO officials, the Director of the Central Intelligence Agency appointed a temporary representative to participate as a voting member in all Panel deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency. The Director of ISOO serves as its Executive Secretary and ISOO staff provide program and administrative support for the Panel.

[30]GAO also asked ISOO officials whether a congressional staff member with a security clearance would be able to submit an appeal to ISCAP. In response to this hypothetical question, ISOO officials expressed the view that the challenge process under the Executive Order was intended to apply to Executive Branch, not Legislative Branch personnel, and therefore an appeal to ISCAP would similarly not be available to congressional staff.

similarly reflect a disagreement about whether a Member of Congress would be considered an "authorized holder."[31]

The ISOO officials also identified the PIDB as the avenue for classification challenges by Members of Congress, as stated in the ISCAP letter.[32] Among other functions, the PIDB reviews and makes recommendations to the President in response to congressional requests, made by a committee of jurisdiction or by a member of such a committee, to declassify or evaluate the proper classification of certain records.[33] Although review by the PIDB in response to a congressional request is discretionary, the PIDB must advise the requestors in a timely manner about whether it intends to conduct a review.[34] According to ISOO officials, following a request, PIDB staff would conduct research and meet with relevant officials, often including several OCAs.

Informal process available to Members. DOD and State have various processes that Members can use to informally challenge the classification of information, including through personal conversations and emails. As

[31]The head of an agency or the Director of ISOO may make a request for the Attorney General to render an interpretation of the Executive Order with respect to any question arising in the course of its administration. Exec. Order No. 13,526, § 6.2(c). We have conveyed DOD's disagreement to ISOO officials.

[32]DOD officials expressed the view that Members of Congress would obtain a quicker response by pursuing a formal classification challenge directly through DOD OCAs rather than with PIDB because the PIDB process would be less efficient and could likely take longer. For example, PIDB would have to refer challenges back to DOD OCAs on any DOD-related matters.

[33]50 U.S.C. § 3355a(b)(5). In its comments, DOD states that the PIDB Bylaws provide procedures for handling congressional requests to declassify certain records or review declinations to declassify specific records. However, the Bylaws have not been updated to fully reflect the current authority of the PIDB under the statute. The review of congressional requests was added in 2004, but initially covered only requests by committees of jurisdiction to declassify information or reconsider declinations to do so. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1102(b) (2004). In 2010, the statute was amended to extend coverage to requests from members of committees of jurisdiction, as well as to evaluation of the proper classification of information. *See* Intelligence Authorization Act for Fiscal Year 2010, Pub. L. No. 111-259, § 365 (2010). Other purposes of the PIDB also generally relate to congressional or public access to national security-related information and the declassification of information. *See, e.g.*, § 3355a(b)(1), (2), (3).

[34]*See* §§ 3355b(e), 3355d(f). However, under § 3355b(e)(1), if requested by the President, the PIDB must review records or declinations to declassify records that were the subject of a congressional request. Any recommendations the PIDB submits to the President must also be submitted to the Chairman and Ranking Member of the committee that made the request.

mentioned above, DOD and State generally encourage resolving classification issues informally before pursuing a formal classification challenge. According to DOD and State officials, Members and their congressional staff can contact both departments through their respective Legislative Affairs offices to informally question the classification of information. For example, DOD officials explained that congressional staff have contacted DOD informally about the classification of information. Specifically, congressional staff members have requested by phone whether classified information can be shared at a different classification level to facilitate distribution of the information to other staff or to the public. Additionally, State officials noted that when they receive an informal request, State will coordinate with the Bureau of Legislative Affairs and the relevant OCA or the Bureau of Diplomatic Security, which can review how to resolve the informal request. State officials told us that State has not received an informal request by a Member during 2017 through 2020.

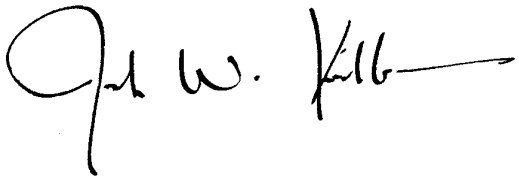
Agency Comments

We provided a draft of this report to DOD, State, NARA and ISOO for review and comment. DOD, NARA and ISOO provided technical comments, which we incorporated into this report as appropriate. DOD and NARA's comments are reprinted in their entirety in appendices I and II.

We are sending copies of this report to the appropriate congressional committees. We are also sending copies to the Secretaries of Defense, State, Secretary of Senate, and Director of the Information Security Oversight Office. In addition, this report will be available at no charge on our website at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at 202-512-9971 or KirschbaumJ@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Sincerely yours,



Joseph W. Kirschbaum
Director, Defense Capabilities & Management

Appendix I: Comments from the Department of Defense

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE
AND SECURITY

March 24, 2021

Dr. Joe Kirschbaum
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Dr. Kirschbaum,

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-21-294, "NATIONAL SECURITY: DOD and State Have Processes for Formal and Informal Challenges to the Classification of Information," dated February 26, 2021 (GAO Code 104147). As the DoD lead for this engagement, my staff completed a review of the GAO Draft Report and offers the following additional comments.

- The Under Secretary of Defense for Intelligence and Security is responsible for implementing and supplementing the requirements of Executive Order (E.O.) 13526 for the DoD.

- The Department is committed to working with members of Congress and congressional committees regarding effective oversight and transparency. As such, DoD recognizes a Congressional member as an "authorized holder" of classified information per E.O. 13526, "Classified National Security Information." Therefore, as an "authorized holder," the member of Congress may challenge the classification of information in their possession to its original classification authority. Neither the National Security Council Director for Records Access and Information Security (RAIS) Management nor the Director, Information Security Oversight Office (ISOO) has issued guidance indicating that an "authorized holder" excludes a member of Congress.

- E.O. 13526 also established the Interagency Security Classification Appeals Panel (ISCAP), which is a Presidential appellate panel to advise and assist the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States per E.O. 13526. The Panel has six standing members, one each from the DoD, State, and Justice, the National Archives and Records Administration (National Declassification Center), the Office of the Director of National Intelligence, and the National Security Advisor (Director for Records Access and Information Security Management). The Director, ISOO is the Executive Secretary of the Panel and oversees the Panel's support staff. The ISCAP members perform four critical functions: 1) **decide on appeals associated with classification challenges**; 2) approve, deny, or amend exemptions from automatic declassification;

- 3) **decide on mandatory declassification review appeals**; and 4) inform senior agency officials and the public on Panel decisions on appeals. I am DoD's primary member on the ISCAP, and my Director, Critical Technology Protection, and the Chief, Classified Information Management and Declassification are alternate members. The ISCAP appeal procedures reinforce the classification challenge processes exercised by DoD (and State) for members of Congress as "authorized holders" of classified information.

- The Public Interest Declassification Board's (PIDB) purpose is to promote the fullest possible public access to a thorough, accurate, and reliable documentary record of significant U.S. national security decisions and activities. The PIDB advises the President and other executive branch officials on the identification, collection, review for declassification, and release of declassified records and materials of archival value. The PIDB also advises the President and other executive branch officials on policies deriving from the issuance by the President of Executive Orders regarding the classification and declassification of national security information. Article VIII of the PIDB bylaws provides procedures for handling congressional requests to declassify certain records or to review declinations to declassify specific records, but this is not the same as processing or deciding an appeal to a classification challenge from a member of Congress.

As stated in DoD policy on the Provision of Information to Congress, it is essential to the proper functioning of the U.S. Government that Congress receives adequate information concerning all Government programs and operations. Accordingly, my office will make every effort to facilitate resolving classification concerns submitted by members of Congress through established Departmental and interagency processes. Given the different views among the Departments of Defense and State, and ISOO as to whether a member of Congress is or is not an authorized holder per E.O. 13526, DoD requests GAO clarify the issue with the Attorney General per E.O. 13526 or with the National Security Council, Director RAIS Management. My point of contact for this matter is Mrs. Donna Rivera, who may be reached at (703) 692-3729 or donna.e.rivera.civ@mail.mil.

Sincerely,

REID.GARRY.PAUL.1072277860 Digitally signed by REID.GARRY.PAUL.1072277860 Date: 2021.03.24 13:44:03 -04'00'

Garry P. Reid
Director for Defense Intelligence
Counterintelligence, Law Enforcement, & Security

2

Appendix II: Comments from the National Archives and Records Administration

Archivist *of the*
United States

19 March 2021

Dr. Joseph Kirschbaum
Director, Defense Capabilities and Management
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Dr. Kirschbaum:

Thank you for the opportunity to comment on the draft report, National Security: DOD and State Have Processes for Formal and Informal Challenges to the Classification of Information (GAO-21-294). My staff in the Information Security Oversight Office have provided technical comments to clarify the report.

If you have any questions regarding this memo, please contact Kimm Richards, NARA's Audit Liaison at 301-837-1668 or via email at kimm.richards@nara.gov.

Sincerely,

DAVID S. FERRIERO
Archivist of the United States

DAVID S. FERRIERO • T: 202.357.5900 • F: 202.357.5901 • *david.ferriero@nara.gov*
National Archives *and* Records Administration • 700 Pennsylvania Avenue, NW • Washington, DC 20408 • *www.archives.gov*

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contact

Joe Kirschbaum, 202-512-9971 or KirschbaumJ@gao.gov

Staff Acknowledgements

In addition to the contact named above, Erika Prochaska (Assistant Director), Yee Wong (Analyst-in-Charge), Suzanne Kaasa, Anastasia Kouloganes, Amie Lesser, Steven Putansu, Clarice Ransom, and Mike Shaughnessy made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Acting Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548