Congressional Research Service
Informing the legislative debate since 1914

Covert Action and Clandestine Activities of the Intelligence Community: Selected Congressional Notification Requirements

Updated July 10, 2023

Congressional Research Service
https://crsreports.congress.gov
R45191

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Section 3091 of Title 50, *U.S. Code* requires the President of the United States to ensure that the congressional intelligence committees are "kept fully and currently informed of the intelligence activities of the United States, including any significant *anticipated* intelligence activity," significant intelligence failures, illegal intelligence activities, and financial intelligence activities.

In fulfilling this statutory requirement, the President must notify Congress of all *covert actions* and significant *clandestine* activities of the Intelligence Community (IC). Congress's interest in being kept informed of these activities originated from instances in the 1970s when media disclosure of past intelligence abuses during times of relatively limited congressional oversight underscored the importance of Congress taking a more active role. Over time, these notification requirements were written into statute or became customary.

Covert action is codified in Title 50, *U.S. Code* as an intelligence activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States will not be apparent or acknowledged publicly. The term *clandestine* describes a methodology used for a range of sensitive intelligence and military activities—conducted under Title 50 or Title 10 *U.S. Code* authority—in which the activity itself, as well as U.S. sponsorship, is secret. Congress's particular interest in these activities is, in part, due to the characteristics that they have in common: they involve particularly sensitive sources and methods, have significant implications for U.S. foreign relations, and incur serious risk of damage to U.S. national security or loss of life in the event of exposure or compromise.

Different committees exercise oversight jurisdiction depending upon how a particular activity is defined and the statutory authority under which it is conducted. Most intelligence activities, to include covert action, are authorized under Title 50, *U.S. Code.* Title 10, *U.S. Code* provides authorities for the military, to include clandestine activities of the military.

The President and intelligence committees are responsible for establishing the procedures for notification, which are generally to be done in writing. Partly in deference to this higher standard, such notifications are sometimes limited to specific subgroups of Members of the Senate and the House of Representatives in certain circumstances, as defined by law and custom.

This report is accompanied by two related reports: CRS Report R45175, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions*, by Michael E. DeVine, and CRS Report R45196, *Covert Action and Clandestine Activities of the Intelligence Community: Framework for Congressional Oversight In Brief*, by Michael E. DeVine.

Contents

Contacts

Non-Covert Action Intelligence Activities

Section 3092 of Title 50, *U.S. Code*, requires that the Director of National Intelligence and the head of any element of the intelligence community keep the congressional intelligence committees "fully and currently informed" of all intelligence activities other than covert action. Intelligence Community Directive (ICD) 112, *Congressional Notification*, specifies that it is the specific IC element that determines which activities are reportable.[1] Some notifications, by their nature, are after-the-fact, such as a significant intelligence failure "extensive in scope, continuing in nature" affecting U.S. national security.[2] Examples of significant activities, including significant *anticipated* intelligence activities that are reportable include

1. Intelligence activities that entail, with reasonable foreseeability, significant risk of exposure, compromise, and loss of human life;
2. Intelligence activities that are expected to have a major impact on important foreign policy or national security interests;
3. A potentially pervasive failure, interruption, or compromise of a collection capability or collection system;
4. Deployment of new collection techniques that represent a significant departure from previous operations or activities or that result from evidence of significant foreign developments;
5. Significant activities undertaken pursuant to specific direction of the President or the National Security Council (other than covert action); or
6. Significant developments in, or the resolution of, a matter previously reported.[3]

Notification

Generally, notifications shall be made within 14 days of a "final determination … that a significant activity should be reported" to Congress.[4] They should be in writing and include the nature of the circumstances and an explanation of their significance.[5]

Sensitive Intelligence Activities Other Than Covert Action

Typically, intelligence activities considered routine and less sensitive are briefed to the membership of the two congressional intelligence committees, the House Permanent Select Committee on Intelligence (HPSCI), and the Senate Select Committee on Intelligence (SSCI) in accordance with applicable statutes and Intelligence Community Directive-112 (ICD-112), *Congressional Notification*. In certain circumstances the notification requirement established by 50 U.S.C. §3092 may be met through oral briefings provided to the chairs of the two congressional intelligence committees, the ranking member of the HPSCI, and the vice chair of

[1] Oral notifications shall be followed by a written notification. See Intelligence Collection Directive (ICD) 112, *Congressional Notification,* June 29, 2017 at https://www.dni.gov/files/documents/71017/6-29-17_ICD-112_17-00383_U_SIGNED.PDF. ICD-112 applies to the reporting of intelligence activities to the congressional intelligence committees with the exception of covert action. Congressional notification of covert action is governed by 50 U.S.C. §3093 which does not have an implementing ICD.

[2] Ibid.

[3] Ibid. The reporting criteria outlined in ICD-112 are not exhaustive and encompass more activities than the intelligence activities addressed in this report.

[4] ICD-112(E)(4)(a).

[5] ICD-112(E)(4)(b).

the SSCI—a group sometimes referred to colloquially as the *Four Corners*, or the *Gang of Four*. Similar notifications pre-date the establishment of the congressional intelligence committees in the 1970s. Briefings were used to inform relevant congressional committee leadership of especially sensitive intelligence matters, including both covert action and routine intelligence collection programs. Observers characterized them as being oral, often cursory, and limited to committee chairmen and ranking members, plus one or two senior staff members.[6]

Notification

Provision of *Four Corners* or *Gang of Four* notifications is not a statutory requirement, and is not referenced in the rules of either of the two congressional intelligence committees. Reportedly, the leadership and Members of the intelligence committees have accepted this practice in circumstances where the executive branch believes a non-covert action intelligence activity warrants restricted notification in order to reduce the risk of disclosure, inadvertent or otherwise.[7]

Covert Action

Covert action is defined in Title 50 of the *U.S. Code* as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States will not be apparent or acknowledged publicly."[8]

The President may authorize the conduct of a covert action only if he or she determines such an action is "necessary to support identifiable foreign policy objectives of the United States, and is important to the national security of the United States."[9]

Section 3093 of Title 50, *U.S. Code* sets out how the congressional intelligence committees are to be informed of covert actions, to include the use of cyber capabilities when employed in a covert action.[10]

Notification

The President must notify the congressional intelligence committees via a "finding" as soon as possible after approving a covert action.[11] Findings must be made in writing unless the President determines immediate action is required. If time constraints prevent prior notification, a written finding is required as soon as possible, but not later than 48 hours, after the President authorizes a

[6] See David M. Barrett, *The CIA and Congress: The Untold Story from Truman to Kennedy* (Lawrence, KS: University Press of Kansas, 2005), pp. 100-103. See also L. Britt Snider, *The Agency and the Hill: CIA's Relationship with Congress, 1946-2004*, (Washington D.C.: CIA Center for the Study of Intelligence, 2008), p. 281, and Frank J. Smist, *Congress Oversees the Intelligence Community*, 2nd ed. (Knoxville: University of Tennessee Press, 1994), p. 119.

[7] Vicki Divoll, "Congress's Torture Bubble," *The New York Times*, May 12, 2009, at https://www.nytimes.com/2009/05/13/opinion/13divoll.html.

[8] 50 U.S.C. §3093(e). See also CRS Report R45175, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions*, by Michael E. DeVine.

[9] See 50 U.S.C. §3093(a). 50 U.S.C. §3093(e) specifies that such covert actions do not include (1) activities with the primary purpose of acquiring intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of U.S. government programs, or administrative activities; (2) traditional diplomatic or military activities or routine support to such activities; (3) traditional law enforcement activities conducted by U.S. government law enforcement agencies or routine support to such activities; or (4) activities to provide routine support of any other overt activities of other U.S. government agencies abroad.

[10] The statute governing notification requirements for cyber capabilities when employed as a covert action can be found in 10 U.S.C. §396(c)(2). This statute references the notification requirements for covert action generally under 50 U.S.C. §3093.

[11] 50 U.S.C. §3093(a) and (c)(1).

particular covert action.[12] Findings may not be used to authorize or sanction a covert action, or any aspect of any such action, that already has occurred.[13] Nor may they be used to authorize any action that would violate the Constitution or any statute of the United States.[14]

Findings are to specify each department, agency, or entity of the U.S. government authorized to fund or otherwise participate in any significant way in the activity.[15] They also are to specify whether it is contemplated that any third party that is not an element of, or a contractor or contract agent of the U.S. government, or that is not otherwise subject to U.S. government policies and regulations, will be used to fund or otherwise participate in any significant way, or be used to undertake the covert action on behalf of the United States.[16] The President is also required to keep the congressional intelligence committees informed of any significant change to a previously approved finding or any development involving a significant risk of loss of life, expansion of existing authorities, expenditure of significant funds or resources, risk of compromise of intelligence sources or methods, or a foreseeable risk of serious damage to U.S. diplomatic relations.[17]

Restricted Notifications of Covert Action

If the President determines that it is "essential" to limit access to a covert action finding in order to "meet extraordinary circumstances affecting vital interests of the United States," he may limit the notification of such a presidential finding to the chairs and ranking Members of the House and Senate intelligence committees, the Speaker and Minority Leader of the House of Representatives, and the majority and minority leaders of the Senate. These Members are colloquially known as the *Gang of Eight.*[18]

Whenever such a restricted notification is given, the President is further required to "fully inform" the congressional intelligence committees in a "timely fashion" of the relevant finding, and is further required to provide a statement summarizing the rationale for not providing prior notice of the relevant finding.[19] After 180 days, the President is required either to provide all Members of the intelligence committees with access to the *finding* or explain why access must remain limited.[20]

[12] 50 U.S.C. §3093(a)(1).

[13] 50 U.S.C. §3093(a)(2).

[14] 50 U.S.C. §3093(a)(5).

[15] Although historically covert action is most closely associated with the Central Intelligence Agency (CIA), the statutory definition allows for other departments and agencies of the U.S. government, including the Department of Defense, to conduct covert action as well. See 50 U.S.C. §3093(a)(3).

[16] 50 U.S.C. §3093(a)(4).

[17] 50 U.S.C. §3093(d)(1)-(2).

[18] 50 U.S.C. §3093(c)(2). The statute also allows, at the discretion of the President, notification of "other... members of the congressional leadership" than those specified. Although not addressed in statute, *Gang of Eight* notifications are also made for instances of particularly sensitive intelligence activities other than covert action.

[19] 50 U.S.C. §3093(c)(3).

[20] 50 U.S.C. §3093(c)(5).

Sensitive DOD Activities

The four congressional defense committees exercise oversight of sensitive Department of Defense (DOD) activities.[21] These activities, on occasion, may appear similar to clandestine activities or covert action conducted by the intelligence community. However, they differ in that they are conducted under a military chain of command, generally in support of, or in anticipation of a military operation or campaign conducted under Title 10 authority.[22]

DOD's requirements for notifying Congress differ from those of the intelligence community. Greater integration of military and intelligence activities—desirable from an operational standpoint—has presented challenges when determining whether they fall primarily under Title 10 or Title 50 authority.[23] Moreover, prior notification, which is generally required for covert action and significant *anticipated* intelligence activities, is not typical of congressional notifications of sensitive DOD activities conducted in support of a larger military operation.

Following are the various categories of sensitive military activities that, from an operational standpoint, may appear similar to—and could potentially be confused with—covert action or clandestine activities of the intelligence community. Notification requirements vary depending upon the type of activity and whether it is conducted under Title 10 or Title 50 authority.

Traditional Military Activities

Traditional military activities are referenced but not defined in statute. They have been described as military activities *"under the direction and control of a United States military commander ... preceding and related to hostilities which are either anticipated ... or ... ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly."*[24] Traditional military activities can be conducted covertly (i.e., U.S. sponsorship is secret and unacknowledged) or clandestinely (i.e., the activity itself is secret) in support of the overall military operation. Some have maintained that because these activities can resemble covert action in that they can influence political, military or economic conditions abroad, they warrant greater

[21] For purposes of Title 10, the four congressional defense committees include the Armed Services and Appropriations committees of the Senate and House (10 U.S.C. §101(a)(16)). Section 1(a) of H.Res. 658, 95th Cong., 1st sess. (1977) provides for one member from each of the House defense committees to also be a member of the House Permanent Select Committee on Intelligence (HPSCI). Section 2(a)(1) of S.Res. 400, 94th Cong. 2nd sess. (1976) provides for one member from each party from each of the Senate defense committees to be a member of the SSCI.

[22] Although the CIA is commonly associated with covert action, 50 U.S.C. §3093 allows for other departments of the executive branch, such as DOD, to conduct covert action. In the event DOD conducts an operation as a covert action, it would be done under a military chain of command. For example, military activities known as *other-than-routine support* to traditional military activities, fall under 50 U.S.C. §3093 governing covert action. See CRS Report R45175, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions*, by Michael E. DeVine.

[23] For a more detailed description of Title 10 and Title 50 authorities, see CRS Report R45175, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions*, by Michael E. DeVine. See also, Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," Harvard National Security Journal, Harvard University Law School (Cambridge: December 2, 2011). Wall argues that Titles 10 and 50 "create mutually supporting, not mutually exclusive, authorities." See also Joseph B. Berger III, "Covert Action: Title 10, Title 50, and the Chain of Command," JFQ, Issue 67, 4th Quarter 2012. Berger and others address the potential hazards that may present themselves when conducting activities under Title 50 authority that risk exposing members of the Armed Forces to an adversary's denial of their prisoner-of-war status under the Geneva Convention Relative to the Treatment of Prisoners of War.

[24] See U.S. Congress, House of Representatives, *Intelligence Authorization Act, Fiscal Year 1991*, conference report to accompany H.R. 1455, 102nd Cong., 1st sess., July 25, 1991, H.Rept. 102-166, pp. 29-30.

oversight.[25] In statute traditional military activities and routine support to these activities are specifically exempt from the congressional notification requirements for covert action.[26] Statutory requirements for notifying Congress depend upon the specific category of traditional military activity and the overall military operation or campaign that it supports.

Operational Preparation of the Environment

Operational Preparation of the Environment (OPE) is a category of traditional military activity, defined in DOD doctrine—not in statute—as "the conduct of activities in likely or potential operational areas to set conditions for mission execution."[27] OPE can be conducted covertly or clandestinely and often involves the employment of U.S. Special Operations Forces (SOF) in counterterrorism operations. Examples of OPE could include close-in reconnaissance of a target, infrastructure development in a targeted area, or the reception, staging, onward movement and integration of forces in an anticipated area of operations. Congress previously has expressed concern that the military overuses the term *OPE* resulting in these operations effectively circumventing oversight by the congressional intelligence committees. *OPE can also include clandestine intelligence collection, conducted by the U.S. Armed Forces*, for example, which, as part of a larger military operation, might neither be brought to the attention of the congressional intelligence committees, nor be given proper oversight by the congressional defense committees.[28]

Notification

Because the military conducts OPE as a category of traditional military activities, these operations are not subject to congressional notification as a covert action or significant anticipated intelligence activity. The Assistant Secretary of Defense for Low Intensity Conflict is required to brief the congressional defense committees quarterly on any clandestine activities, the sum total of which do not exceed $15 million dollars, which the Secretary "determines to be proper for preparation of the environment for operations of a confidential nature."[29]

Routine Support to Traditional Military Activities

Routine support to traditional military activities may include logistic support to impending or ongoing military operations that involve U.S. Armed Forces unilaterally and in which the U.S. role is generally acknowledged.[30] Despite the acknowledgement of the overall U.S. role, specific

[25] See Joel Myer, "Supervising the Pentagon: Covert Action and Traditional Military Activities in the War on Terror," *Administrative Law Review*, Vol. 59, No. 2, Spring 2007.

[26] See 50 U.S.C. §3093(e): "... the term 'covert action'... does not include ... traditional diplomatic or military activities or routine support to such activities."

[27] See Joint Staff, "DOD Dictionary of Military and Associated Terms," November 2021 revision, p. 161, at https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf.

[28] See U.S. Congress, House of Representatives, "Intelligence Authorization Act for Fiscal Year 2010," conference report, together with minority and additional views to accompany H.R. 2701, 111th Cong., 1st sess., June 26, 2009, pp. 48-49: "Clandestine military intelligence-gathering operations, even those legitimately recognized as OPE, carry the same diplomatic and national security risks as traditional intelligence-gathering activities. While the purpose of many such operations is to gather intelligence, DOD has shown a propensity to apply the OPE label where the slightest nexus of a theoretical, distant military operation might one day exist. Consequently, these activities often escape the scrutiny of the intelligence committees, and the congressional defense committees cannot be expected to exercise oversight outside of their jurisdiction."

[29] 10 U.S.C. §127f(a); 10 U.S.C. §127f(e).

[30] Joint Explanatory Statement of the Committee of Conference, H.R. 1455, July 25, 1991.

routine support activities may be conducted clandestinely (i.e., the activity is secret) or covertly (i.e., the U.S. role in the specific activity is unacknowledged).

Notification

The association of these activities to a supported military operation in which the U.S. role is acknowledged statutorily exempts these activities from congressional notification as a covert action.[31] DOD generally provides notification to Congress as part of the hearings and briefings associated with the specific military activity or operation that is being provided routine support.

Other-than-Routine Support to Traditional Military Activities

Other-than-routine support to traditional military activities includes activities abroad that involve other than unilateral employment of U.S. forces. They may be conducted covertly and clandestinely (i.e., the activity as well as U.S. sponsorship are secret and may not be acknowledged). They include recruitment of, training for, or other assistance to non-U.S. individuals, organizations or populations to conduct activities—wittingly or not—that support U.S. military objectives.

Notification

Because they may be conducted well in advance of an anticipated military operation and because they can be intended to influence political, economic or military conditions in another country[32]—such as swaying public opinion—*other-than-routine support* to traditional military activities is subject to congressional notification for covert action under 50 U.S.C. §3093.[33]

---

[31] 50 U.S.C. §3093(e)(2).

[32] That is, the activities may precede National Command Authority approval for hostilities or operational planning for hostilities. See U.S. Congress, House of Representatives, *Intelligence Authorization Act, Fiscal Year 1991*, conference report to accompany H.R. 1455, 102nd Cong., 1st sess., July 25, 1991, H.Rept. 102-166, pp. 29-30.

[33] See S. Rep. No. 101-358, p. 55:

> [T]he Committee would regard as 'other-than routine' support *(requiring a finding and reporting to the committee)* such activities as clandestinely recruiting and/or training of foreign nationals with access to the target country actively to participate in and support a U.S. military contingency operation; clandestine efforts to influence foreign nationals of the target country concerned to take certain actions in the event a U.S. military contingency operation is executed; clandestine efforts to influence and effect public opinion in the country concerned where U.S. sponsorship of such efforts is concealed; and clandestine efforts to influence foreign officials in third countries to take certain actions in the event a U.S. military contingency operation is executed. (Traditional diplomatic activities would be excluded by other parts of this section.)
>
> In other words, the Committee believes that when support to a possible military contingency operation involves other than unilateral efforts by U.S. agencies in support of such operation, to include covert U.S. attempts to recruit, influence, or train foreign nationals, either within or outside the target country, to provide witting support to such operation, should it occur, such support is not "routine." *In such circumstances, the risks to the United States and the U.S. element involved have, by definition, grown to a point where a substantial policy issue is posed, and because such actions begin to constitute efforts in and of themselves to covertly influence events overseas* (as well as provide support to military operations). [emphasis added]

See also, Joel T. Meyer, "Supervising the Pentagon: Covert Action and Traditional Military Activities in the War on Terror," *Administrative Law Review* (Washington, DC: The American University, 59 Admin, L. Rev. 463 (2007)).

Military Cyber Operations Not Constituting Covert Action

Cyber Weapons

Section 396 of Title 10 of the *U.S. Code* describes the use of cyber capabilities "intended for use as a weapon" that specifically do not constitute covert action.[34]

Notification

For these operations, the Secretary of Defense must notify the congressional defense committees in writing

- Within 48 hours of the use of a cyber weapon that has been approved for use under international law;
- On a quarterly basis for any cyber capability developed for use as a weapon;[35] and
- Immediately—"to the maximum extent practicable"—following the unauthorized disclosure of a cyber weapon capability.

Clandestine Military Activities or Operations in Cyberspace

Section 1632 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232) amended Section 394 of Title 10 of the *U.S. Code* by providing statutory authority for DOD to conduct clandestine military activities or operations in cyberspace as a type of traditional military activity.[36] The act defined clandestine military activity or operation in cyberspace as

> a military activity or military operation carried out in cyberspace, or associated preparatory actions, authorized by the President or the Secretary [of Defense] that is marked by, held in, or conducted with secrecy, where the intent is that the activity or operation will not be apparent or acknowledged publicly, and is to be carried as part of a military operation plan approved by the President or the Secretary in anticipation of hostilities or as directed by the President or Secretary; to deter, safeguard, or defend against attacks or malicious cyber activities against the United States or Department of Defense information, networks, systems, installations, facilities, or other assets; or in support of information related capabilities.[37]

---

[34] Section 396(c)(2) specifies that covert action is an exception to these notification requirements.

[35] This measure expands Congress's oversight role and ensures that the intended use of cyber weapons is consistent with emerging legal norms. See Benjamin Dynkin and Barry Dynkin, "Cybersecurity Showdown: Why the Military is Preparing for a New Kind of War," *The National Interest*, January 9, 2018.

[36] Section 1632(3)(b)-(c) of P.L. 115-232:

> (b) Affirmation of Authority.—Congress affirms that the activities or operations referred to in subsection (a), when appropriately authorized, include the conduct of military activities or operations in cyberspace short of hostilities (as such term is used in the War Powers Resolution (P.L. 93-148; 50 U.S.C. 1541 et seq.)) or in areas in which hostilities are not occurring, including for the purpose of preparation of the environment, information operations, force protection, and deterrence of hostilities, or counterterrorism operations involving the Armed Forces of the United States.
>
> (c) Clandestine Activities or Operations.—A clandestine military activity or operation in cyberspace shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 U.S.C. 3093(e)(2)).

[37] Ibid. Some internal numbering omitted.

The congressional intent of this language was partly to provide DOD greater latitude to conduct operations in cyberspace under the military's Title 10 authorities without the greater oversight requirements of covert action.[38]

Notification

Title 10 U.S.C. §484(a) requires the Under Secretary of Defense for Policy, the Commander of United States Cyber Command, and the Chairman of the Joint Chiefs of Staff, or their designees to provide the congressional defense committees quarterly briefings "on all offensive and significant defensive military operations in cyberspace, including clandestine cyber activities, carried out by the Department of Defense during the immediately preceding quarter."[39] The briefings are to include the command involved, descriptions of the operations, an overview of the legal authorities under which the operations took place, critical operational challenges posed by major adversaries or otherwise encountered, and an overview of the readiness of the Cyber Mission Forces to perform assigned missions.[40]

Sensitive Military Operations

Sensitive Military Operations are defined in Section 130f(d)(1)-(3) of Title 10 *U.S. Code* as (1) "a lethal operation or capture operation" conducted either by the U.S. Armed Forces or a foreign partner in coordination with the U.S. Armed Forces that targets a specific individual or individuals; or (2) an operation conducted by the U.S. Armed Forces in self-defense or in defense of foreign partners, including a cooperative U.S.-foreign operation; or (3) an operation conducted by the U.S. Armed Forces to free an individual from the control of hostile foreign forces.

Notification

The Secretary of Defense is to submit notice in writing to the congressional defense committees

- Within 48 hours of the operation, or within 48 hours of providing verbal notice to Congress;
- Immediately—"to the maximum extent practicable"—following an unauthorized disclosure of an operation, or within 48 hours of providing verbal notice to Congress;

---

[38] The law's conference report explained the reasoning for classifying these types of cyber operations as traditional military activities by noting the difficulties DOD previously encountered in obtaining approval for cyberspace operations. See U.S. Congress, House of Representatives Committee on Armed Services, *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, P.L. 115-232, conference report to accompany H.R. 5515, 115th Cong., 2nd sess., July 25, 2018, H.Rept. 115-874:

> One of the challenges routinely confronted by the Department is the perceived ambiguity as to whether clandestine military activities and operations, even those short of cyber attacks, qualify as traditional military activities as distinct from covert actions requiring a Presidential Finding. As a result, with respect to actions that produce effects on information systems outside of areas of active hostilities, the Department of Defense has been limited to proposing actions that could be conducted overtly on attributable infrastructure without deniability—an operational space that is far too narrow to defend national interests. The conferees see no logical, legal, or practical reason for allowing extensive clandestine traditional military activities in all other operational domains (air, sea, ground, and space) but not in cyberspace. It is unfortunate that the executive branch has squandered years in interagency deliberations that failed to recognize this basic fact and that this legislative action has proven necessary.

[39] 10 U.S.C. §484(a).

[40] 10 U.S.C. §484(b)(1)-(5).

- "Periodically" on DOD personnel and equipment assigned to sensitive military operations, including DOD support to such operations conducted under Title 50 authorities.[41]

Sensitive Military Cyber Operations

Sensitive military cyber operations are a subcategory of sensitive military operations. Congress defines sensitive military cyber operations under Title 10 as operations carried out by the Armed Forces of the United States that are intended to cause cyber effects against a foreign terrorist organization or country, including its armed forces and proxy forces, with which the United States is not engaged in hostilities, or with respect to which the involvement of the United States in hostilities has not been acknowledged publicly, which involve a medium to high degree of impact on the intended objective.[42] DOD has identified two subcategories of sensitive military cyber operations, neither of which is defined in statute. The first, offensive cyberspace operations, is defined by DOD as "missions intended to project power in and through cyberspace."[43] The second, defensive cyberspace operations, is defined by DOD as "missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity."[44]

Notification

Depending upon the specific operation, Sensitive Military Cyber Operations could be either conducted as a type of traditional military activity or—if accompanied by a presidential finding and conducted under Title 50 authority—as a covert action.[45] For those conducted as a traditional military activity, the Secretary of Defense is to notify the congressional defense committees

- In writing within 48 hours of the operation taking place;[46] or
- Immediately—"to the maximum extent practicable"—subsequent to an unauthorized disclosure of a sensitive military cyber operation. In the event the initial notification is verbal, a written notification "signed by the Secretary, or the Secretary's designee," shall be provided not later than 48 hours afterwards.[47]

[41] 10 U.S.C. §130f(a)-(c).

[42] 10 U.S.C. §395(c)(1)(A)-(B).

[43] Offensive cyberspace operations are defined in Joint Pub 3-12, *Cyberspace Operations*, p. GL-5. See also note to §111 of Title 10 U.S.C., P.L. 112-81, div. A, title IV, §954, 125 Stat. 1551: "Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests subject to (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution (50 U.S.C. §1541 et seq.)."

[44] Currently, statute does not define or describe offensive or defensive cyberspace operations. JP 3-12 p. GL-4 defines defensive cyberspace operations as "missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity."

[45] 10 U.S.C. §395(d)(2). "The notification requirement [for the Secretary of Defense to notify the congressional defense committees in writing within 48 hours of a sensitive military cyber operation] does not apply ... to a covert action." [some internal numbering omitted]

[46] 10 U.S.C. §395(a).

[47] 10 U.S.C. §395(b)(3).

Defense Clandestine Service Activities

Under Title 10, *U.S. Code*, the Defense Clandestine Service, subordinate to the Defense Intelligence Agency, provides dedicated clandestine support to the DOD to meet unique military intelligence collection priorities and to provide unique capabilities to the intelligence community.[48]

Notification

The Secretary of Defense is to provide to the defense and intelligence committees of the House and Senate quarterly briefings on the deployments and collection activities of personnel of the Defense Clandestine Service.[49]

Counterterrorism Operations

DOD is required to keep Congress informed of U.S. counterterrorism operations and related activities. Along with the initial notification, DOD must update information on any counterterrorism activities within each geographic combatant command; how these activities support the respective theater campaign plan; overviews of the authorities and legal issues, as well as any related interagency activities; and any other matters the Secretary of Defense considers appropriate.[50]

Notification

In statute, DOD is required to provide monthly briefings to the congressional defense committees on U.S. counterterrorism and related activities that are not conducted as a covert action.[51]

Issues for Congress

- Congress may consider whether existing inter-committee coordination mechanisms ensure the congressional intelligence committees are sufficiently informed of particular clandestine activities, such as sensitive military cyber operations, which fall under the jurisdiction of the congressional armed services committees.
- The term "other-than-routine-support" to traditional military activities currently is not defined in statute. Congress may consider during its consideration of the IAA whether there is sufficient clarity on the character of these activities to warrant an amendment to the definition of covert action to specifically include the term "other-than-routine-support to traditional military activities."

[48] 10 U.S.C., note prec. §421.

[49] Ibid.

[50] 10 U.S.C. §485(a)-(b).

[51] Ibid.

Author Information

Michael E. DeVine
Analyst in Intelligence and National Security

Acknowledgments

This report was originally coauthored by Heidi M. Peters, former CRS Analyst in U.S. Defense Acquisition Policy.

Disclaimer