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

Updated July 2, 2019

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 benign 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 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 10 or Title 50 *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 in Brief*, 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 Intelligence Activities Notifications

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

Non-Covert Intelligence Activities: *Gang of Four* Notifications

Typically, intelligence activities that are considered less sensitive are briefed to the membership of each committee in line with statute and ICD-112. In certain circumstances, however, the Section 3092 requirement may be met through notifications to select members of the House and Senate, a group colloquially known as the *Gang of Four*. *Gang of Four* intelligence notifications are usually oral briefings provided only to the chairs and ranking members of the two congressional intelligence committees.

Gang of Four notifications are not codified in statute; nor do they figure in the rules of either of the two congressional intelligence committees. They are a practice generally accepted by the leadership of the intelligence committees in circumstances when the executive branch believes a

[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.

non-covert action intelligence activity—often a collection program—to be of such sensitivity that a restricted notification is warranted in order to reduce the risk of disclosure, inadvertent or otherwise. These notifications are provided as briefs without any written record or notetaking.

Gang of Four notifications pre-date the establishment of the congressional intelligence committees in the 1970s. Similar briefings were earlier used to inform relevant congressional committee leadership of especially sensitive intelligence matters, including both covert action and routine intelligence collection programs. Observers, commenting on such notifications used during this time period, characterized them as being oral, often cursory, and limited to committee chairmen and ranking members, plus one or two senior staff members.[4]

Covert Action Notifications

Section 3093 of Title 50, *U. S. Code* sets out how the congressional intelligence committees are to be informed of covert actions, to include use of cyber capabilities when employed in a covert action.[5]

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."[6] Such determinations are to be generally set forth in a written *finding* to be reported to the congressional intelligence committees as soon as possible after the approval of a finding, and before the covert action starts.[7]

Findings must be made in writing unless immediate United States action is required. If time constraints prevent the initial preparation of a written *finding*, a written *finding* is to be produced as soon as possible but not later than 48 hours after the authorizing decision was made. *Findings* may not authorize or sanction a covert action, or any aspect of any such action, that already has occurred, and may not authorize any action that would violate the Constitution or any statute of the United States.

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.[8] They also are to specify whether it is contemplated that any third party not an element of, or a contractor or contract agent

[4] 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, DC: Center For the Study of Intelligence, Central Intelligence Agency, 2008), p. 281. See also Frank J. Smist, Jr., *Congress Oversees the United States Intelligence Community, Second Edition, 1947-1994,* (Nashville: The University of Tennessee Press, 1994), p. 119.

[5] 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. Prior to reclassification and renumbering of the *U.S. Code*, §396(c)(2) had been 10 U.S.C. §130k(c)(2).

[6] See 50 U.S.C. §3093. This section once classified as 50 U.S.C. §413b prior to editorial reclassification and renumbering. 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.

[7] See 50 U.S.C. §3093(a) and (c).

[8] 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 §3093(a), Title 50, *U. S. Code*.

of, the U.S. government, or who 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. The DNI and responsible IC element must also keep the congressional intelligence committees informed of any significant change to a *finding* or failure of the covert action.

Covert Action: *Gang of Eight* Notifications

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 *finding* to the chairs and ranking minority 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.*[9]

Whenever such a limited 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.[10] After 180 days, the President must either provide all Members of the intelligence committees with access to the *finding* or explain why access must remain limited.[11]

Distinctions between *Gang of Four* and *Gang of Eight* Notifications

Gang of Four and *Gang of Eight* notifications differ in several ways. A principal difference is that the *Gang of Four* notifications procedure is a more informal process that has been accepted by the leadership of the intelligence committees over time, but does not exist in statute.

In contrast, the *Gang of Eight* procedure is codified in statute,[12] and imposes certain statutory obligations on the executive branch. For example, when employing this particular notification procedure, the President must make a determination that vital U.S. interests are at stake if a notification is to be restricted to the *Gang of Eight* and provide a written statement setting forth the reasons for limiting notification to the *Gang of Eight*, rather than notifying the full membership of the intelligence committees.[13]

Another distinction between the two notification procedures, at least since 1980 when the *Gang of Eight* procedure was first enacted in statute, is that *Gang of Four* notifications generally are limited to non-covert action intelligence activities, including principally but not exclusively intelligence collection programs the IC views as particularly sensitive. In contrast, *Gang of Eight* notifications are statutorily limited to particularly sensitive covert action programs.

Notwithstanding these distinctions, there is no provision in statute that restricts whether and how the chairs and ranking members of the intelligence committees share with committee members

[9] See 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.

[10] See 50 U.S.C. §3093(c)(3).

[11] See 50 U.S.C. §3093(c)(4).

[12] See 50 U.S.C. §3093(c)(2).

[13] 50 U.S.C. §3093(c)(3) does not specify whether such a statement must be in writing, nor does it specify to whom such a statement should be provided.

information pertaining to the intelligence activities that the executive branch has provided only to the committee leadership, either through *Gang of Four* or *Gang of Eight* notifications. Nor, apparently, is there any statutory provision that sets forth any procedures that would govern the access of appropriately cleared committee staff to such classified information.

Some critics of restricted intelligence notification of Congress, such as the *Gang of Eight* procedures, have maintained that they do not allow for effective oversight because participating Members "cannot take notes, seek the advice of their counsel, or even discuss the issues raised with their committee colleagues."[14] Other critics have contended that restricted notifications such as *Gang of Eight* and *Gang of Four* briefings have been "overused."[15] Still others have believed *Gang of Four* notifications are unlawful because they are not based in statute.[16]

Supporters of *Gang of Eight* notifications have asserted that such restricted notifications continue to serve their original purpose, which is to protect operational security of particularly sensitive intelligence activities while they are ongoing. Further, they have pointed out that although Members receiving these notifications may be constrained in sharing detailed information about the notifications with other intelligence committee members and staff, these same Members can raise concerns directly with the President and the congressional leadership and thereby seek to have any concerns addressed.[17] Supporters also have argued that Members receiving these restricted briefings have at their disposal a number of rarely used legislative remedies if they decide to oppose particular programs, including the capability to use the appropriations process to withhold funding.[18]

Sensitive DOD Activities Notifications

The four congressional defense committees exercise oversight of sensitive Department of Defense (DOD) activities.[19] These activities, on occasion, may appear similar to clandestine activities or covert action conducted by the IC. 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.[20]

---

[14] See letter from Representative Jane Harman to President George W. Bush, January 4, 2006, regarding the National Security Agency (NSA) electronic communications surveillance program, often referred to as the Terrorist Surveillance Program, or TSP, at https://votesmart.org/public-statement/148514/harman-says-limited-briefings-on-nsa-program-were-improper#.XQqY1zaWyUl.

[15] See Tim Starks, "Pelosi Controversy Suggests Changes to Congressional Briefings Are Due," Congressional Quarterly, May 14, 2009, at https://plus.cq.com/doc/news-3118085?16&searchId=MmqzZNlB.

[16] See Vicki Divoll, "Congress's Torture Bubble," *New York Times*, May 12, 2009, at https://www.nytimes.com/2009/05/13/opinion/13divoll.html?mtrref=www.google.com&gwh=3B7AAEF6220457EB9030C6D65C47063B&gwt=pay.

[17] See Congressional Quarterly transcript of press conference given by Representative Peter Hoekstra, December 21, 2005.

[18] See Tim Starks, "Pelosi Controversy Suggests Changes to Congressional Briefings are Due," Congressional Quarterly, May 14, 2009, at https://plus.cq.com/doc/news-3118085?16&searchId=MmqzZNlB.

[19] For purposes of Title 10, the four congressional defense committees include the Armed Services and Appropriations committees of the Senate and House, see 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 Senate Select Committee on Intelligence (SSCI).

[20] 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*

Insofar as Congress exercises oversight of these activities, 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.[21] 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 notification requirements for sensitive military activities that, from an operational standpoint, could be confused with covert or clandestine activities of the intelligence community.

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."*[22] 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 oversight.[23] In statute, however, traditional military activities and routine support to these activities are specifically exempted from the congressional notification requirements for covert action.[24] 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 areas of operations to prepare and shape the operational environment."[25] OPE can be conducted covertly or clandestinely and often involves the employment of U.S. Special Operations Forces (SOF) in counterterrorism operations. Joint Publication 3-05 cites examples of OPE as "close-

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 in Brief*, by Michael E. DeVine.

[21] See, for example, 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.

[22] 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.

[23] 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.

[24] 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."

[25] See Joint Staff, "DOD Dictionary of Military and Associated Terms," May 2019 revision, available at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

target reconnaissance … reception, staging, onward movement, and integration … of forces … [and] infrastructure development."[26]

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. Congress has been concerned 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, that falls outside the jurisdiction of congressional defense committees, yet, as part of a larger military operation, might not be brought to the attention of the congressional intelligence committees.[27]

Routine Support to Traditional Military Activities

Routine support to traditional military activities might include logistic support to impending or ongoing military operations which involve U.S. Armed Forces *unilaterally* and in which the U.S. role is generally acknowledged.[28] Despite the acknowledgement of the overall U.S. role, specific 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). Their connection to a supported military activity in which the U.S. role is acknowledged statutorily exempts these activities from congressional notification as a covert action.[29]

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. 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[30]—such as swaying public opinion—*other-than-routine support* to

[26] Joint Publication 3-05, "Special Operations," Joint Staff, July 16, 2014, available at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_05.pdf. Joint Publication 3-05 describes *preparation of the environment* as an "umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operation."

[27] 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."

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

[29] 50 U.S.C. §3093(e)(2).

[30] 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.

traditional military activities is subject to congressional notification for covert action under Section 3093, Title 50 of the *U. S. Code*.[31]

Defense Clandestine Service Activities

Under Title 10, *U. S. Code*,[32] the Defense Clandestine Service, subordinate to the Defense Intelligence Agency, provides dedicated clandestine support to DOD to meet unique military intelligence priorities and to provide unique capabilities to the IC.

The Secretary of Defense shall 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.[33]

Counterterrorism Operations Briefings

Section 485 of Title 10, *U.S. Code* requires the Secretary of Defense to provide monthly briefings to the congressional defense committees that describe DOD counterterrorism operations and related activities. Under the statute, each such briefing must include specific elements

- a global update on activity within each geographic combatant command and how such activity supports the respective theater campaign plan;
- an overview of authorities and legal issues, including limitations;
- an overview of interagency activities and initiatives; and
- any other matters the Secretary considers appropriate.[34]

[31] 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)).

[32] See 10 *U.S. Code*, prec. 421 note.

[33] Ibid.

[34] 10 U.S.C. §485(a)-(b).

Military Cyber Operations (Not Constituting Covert Action)

Cyber Weapons

Section 396 of Title 10 of the *U. S. Code* provides notification requirements for cyber capabilities "intended for use as a weapon" that specifically do not constitute covert action.[35] 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;[36] and
- immediately following the unauthorized disclosure of a cyber weapon capability.

Offensive and Significant Defensive Military Operations in Cyberspace

Offensive cyberspace operations are defined as operations "intended to project power by the application of force in and through cyberspace."[37] Defensive cyberspace operations are defined as active or passive cyberspace operations "to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems."[38] Section 484 of Title 10 *U. S. Code* mandates the Secretary of Defense provide the congressional defense committees written quarterly briefings "on all offensive and significant defensive military operations in cyberspace carried out by the Department of Defense during the immediately preceding quarter." The briefings are to include the command involved and an overview of the legal authorities under which the operations took place.

Sensitive Military Operations

Sensitive Military Operations are defined in Section 130f(d)(A)-(B) of Title 10 *U. S. Code* as (1) kill or capture operations conducted by U.S. Armed Forces or conducted by a foreign partner in coordination with the U.S. Armed Forces that target 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 during a cooperative operation. Sensitive military operations statutorily exclude any operation conducted in Iraq, Syria, or Afghanistan.[39]

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

[35] Prior to reclassification and renumbering of the *U.S. Code*, 10 U.S.C. §396 had been 10 U.S.C. §130k. Section 396(c)(2) specifies that covert action is an exception to these notification requirements.

[36] 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.

[37] See CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary. See also Joint Publication 3-12(R), *Cyberspace Operations* (Washington, DC: Joint Staff, June 8, 2018), p. GL-5, at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

[38] Joint Publication 3-12, *Cyberspace Operations*, (Washington, DC: Joint Staff, June 8, 2018) p. II-3, at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

[39] 10 U.S.C. 130f(2). The statute on sensitive military operations was amended by P.L. 115-232 §103(a) by deleting an unspecific, potentially confusing reference to these operations being conducted "outside a declared theater of active armed conflict." Section 130f(2) removes any geographic uncertainty: Sensitive military operations are operations, as defined in statute, conducted outside of Syria, Iraq, and Afghanistan.

- within 48 hours of the operation (or within 48 hours of providing verbal notice to Congress);
- immediately following an unauthorized disclosure of an operation;
- "periodically" on DOD personnel and equipment assigned to sensitive military operations, including DOD support to such operations conducted under Title 50 authorities. [40]

Sensitive Military Cyber Operations

Sensitive military cyber operations are a subcategory of sensitive military operations. Congress defines *sensitive military cyber operations* in Title 10 *U.S. Code* as operations carried out by the armed forces of the United States that are intended to cause cyber effects outside a geographic location where the Armed Forces of the United States are involved in hostilities or where hostilities have been declared by the United States.[41] Sensitive military cyber operations have two subcategories. The first, offensive cyberspace operations, is not defined in statute, but by DOD, as "missions intended to project power in and through cyberspace." The second, defensive cyberspace operations, is defined in statute as operations "outside of Department of Defense information networks that are aimed at defeating an ongoing or imminent threat."[42] Sensitive military cyber operations do not include training exercises that have effects on foreign states so long as these states concur, nor are they considered covert action.[43]

The Secretary of Defense shall notify the congressional defense committees

- within 48 hours of the operation taking place; or
- immediately subsequent to an unauthorized disclosure of a sensitive military cyber operation.

Author Information

Michael E. DeVine
Analyst in Intelligence and National Security

Acknowledgments

This report was originally coauthored by Heidi M. Peters, CRS Analyst in U.S. Defense Acquisition Policy. CRS also acknowledges the prior research on *Gang of Four* and *Gang of Eight* notifications by former CRS analysts in intelligence and national security, Marshall C. Erwin and Alfred Cumming.

[40] 10 U.S.C. §130f(a)-(c).

[41] 10 U.S.C. §395(c)(1)(A)-(B). Prior to reclassification and renumbering of the *U.S. Code*, the statute governing sensitive military cyber operations had been 10 U.S.C. §130(j).

[42] For the DOD definition of offensive cyberspace operations, see Joint Publication 3-12, *Cyberspace Operations*, June 8, 2018, p. GL-5, at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf. Currently, statute does not define or describe offensive or defensive cyberspace operations consistent with DOD in JP 3-12.

[43] 10 U.S.C. §395(d)(1)-(2).

Disclaimer