NSA/CSS POLICY 12-3

PROTECTION OF CIVIL LIBERTIES AND PRIVACY OF U.S. PERSON INFORMATION WHEN CONDUCTING NSA/CSS MISSION AND MISSION-RELATED ACTIVITIES

DATE:	15 February 2022 (See Document History.)
OFFICE OF PRIMARY INTEREST:	Office of General Counsel (OGC, D2), 963-3121 (secure)
RELEASABILITY:	This policy is approved for public release. The official document is available on the Office of Policy website ("go policy").
AUTHORITY:	Paul M. Nakasone, General, U.S. Army; Director, NSA/Chief, CSS
ISSUED:	10 January 2022

PURPOSE AND SCOPE

1. This document establishes policy and procedures and assigns responsibilities to provide reasonable assurance that *NSA/CSS mission and mission-related activities* (hereafter referred to as "mission activities") are conducted in a manner that protects the constitutional and legal rights and the civil liberties and privacy of *U.S. persons (USPs)* as required by law, Executive orders (E.O.s), Department of Defense (DoD) policies, and internal NSA/CSS policy. The policy specifically implements DoD Directive (DoDD) 5240.01, "DoD Intelligence Activities" (Reference a), in accordance with the provisions of E.O. 12333, "United States Intelligence Activities" (Reference b), as they pertain to NSA/CSS and other Defense Intelligence Components.

2. This policy applies to all *NSA/CSS employees* as defined in this policy while conducting *signals intelligence (SIGINT)*, *cybersecurity*, capabilities development and support, research, or foreign *cryptologic* partnerships. It also applies to all elements of the *United States SIGINT System (USSS)* as herein defined. All mentions of Defense Intelligence Components, or the head of such a component, in NSA/CSS's Attorney General (AG)–approved procedures (DoD Manual (DoDM) 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities" (Reference c; annotated version in Annex A), and the SIGINT Annex, DoDM S-5240.01-A, "Procedures Governing the Conduct of DoD Intelligence Activities: Annex Governing Signals Intelligence Information and Data Collected Pursuant to Section 1.7(c) of E.O. 12333" (Reference d; annotated version in Annex B)), shall be read as referring to NSA/CSS and the Director, NSA/Chief, CSS (DIRNSA/CHCSS), respectively.

POLICY

3. In accordance with E.O. 12333 (Reference b), National Security Directive (NSD) 42, "National Policy for the Security of National Security Telecommunications and Information Systems" (Reference e), and DoDD 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," known as the NSA/CSS Charter (Reference f), NSA/CSS shall conduct these mission activities, or any others as assigned in law, policy, or other issuance:

a. SIGINT. The SIGINT mission of NSA/CSS and the USSS is to collect, process, analyze, produce, and disseminate *SIGINT information* for foreign intelligence and counterintelligence purposes in order to support national and departmental missions as well as support to military operations and the identification of foreign cyber threats to U.S. national security systems (NSS) and critical infrastructure. NSA/CSS shall intentionally collect foreign communications. NSA/CSS may intentionally collect USP communications only pursuant to the Foreign Intelligence Surveillance Act (FISA) (Reference g) or to the procedures contained in DoDM 5240.01 (Reference c) and the SIGINT Annex, DoDM S-5240.01-A (Reference d).

b. Cybersecurity. The cybersecurity mission of NSA/CSS is to discover, prevent, mitigate, and eradicate cyber threats to or vulnerabilities of NSS, DoD, and the Defense Industrial Base (DIB) and to provide products and services to safeguard those information systems. In many circumstances, activities undertaken by NSA/CSS for cybersecurity purposes may also include intelligence activities under DoD authorities. Questions regarding the applicability of DoDM 5240.01 (Reference c) or other authorities referenced in this policy should be directed to the NSA Office of General Counsel (OGC, D2).

1) E.O. 12333 (Reference b) affirms DIRNSA's role as National Manager for NSS as designated and defined in NSD 42 (Reference e). In addition, E.O. 13587, "Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information" (Reference h), designates the Secretary of Defense and DIRNSA/CHCSS as the joint Executive Agent for Safeguarding Classified Information on Computer Networks and supplements the responsibilities and authorities of DIRNSA/CHCSS as the National Manager for NSS under NSD 42 (Reference e). DoD Instruction (DoDI) 8500.01, "Cybersecurity" (Reference i), and other DoD policies direct NSA/CSS to provide a wide array of cybersecurity support and services to DoD components.

2) As authorized by the DoD Chief Information Officer (Reference j), NSA/CSS shares *cybersecurity information* and cyber threat information, network security, and mitigation guidance directly with DIB entities, including technology companies and cybersecurity service providers who support the DIB, and provides cybersecurity assistance to DIB entities and their service providers upon request.

3) DoDI 8560.01, "Communications Security (COMSEC) Monitoring" (Reference k), designates DIRNSA/CHCSS as the DoD focal point for COMSEC monitoring of official U.S. Government telecommunications in accordance with the National Manager responsibilities. COMSEC monitoring is subject to separate AG-approved procedures.

4. NSA/CSS shall protect the constitutional and legal rights and the civil liberties and privacy of USPs during the conduct of mission activities, consistent with the U.S. Constitution. NSA/CSS provides appropriate transparency into the civil liberties and privacy protections applied to mission activities in accordance with Intelligence Community Directive 107, "Civil Liberties, Privacy, and Transparency" (Reference l). mission activities shall be conducted in strict compliance with the law, E.O.s and their implementing procedures, and other applicable policies, directives, or issuances, including the Privacy Act of 1974 (Reference m), where that act applies.

5. Policies and procedures governing mission activities that involve the collection of *operations information* or *operations data* are as follows:

a. All SIGINT activities (e.g., SIGINT, SIGINT support to cybersecurity, testing and training on *electronic surveillance* equipment, and support to military exercises) undertaken by NSA/CSS or the USSS using electronic surveillance and that implicate the privacy expectations in the Fourth Amendment (i.e., communications intelligence (COMINT)) are governed by DoDM 5240.01 (Reference c) and either the SIGINT Annex (Reference d) or FISA (Reference g). SIGINT information collected under FISA (Reference g) that is subject to Foreign Intelligence Surveillance Court–approved procedures shall be handled according to those procedures.

b. All SIGINT activities undertaken by NSA/CSS or the USSS that do not implicate the Fourth Amendment (e.g., direction finding, TechSIGINT (technical SIGINT), ELINT (electronic intelligence), FISINT (foreign instrumentation signals intelligence), non-communications and non-communications related data) are governed by Procedures 1 through 4 of DoDM 5240.01 (Reference c) unless they include COMINT or otherwise implicate the Fourth Amendment.

c. All mission activities undertaken by NSA/CSS or the USSS that acquire *information supporting cryptologic operations* (e.g., information that is publicly available, voluntarily provided from *cooperating sources* (including forensics and commercially purchased data)) are governed by Procedures 1 through 4 of DoDM 5240.01 (Reference c).

d. All COMSEC monitoring activities undertaken by NSA/CSS shall be conducted in accordance with the National Telecommunications and Information Systems Security Directive No. 600, "Communications Security (COMSEC) Monitoring" (Reference n), and all applicable NSA/CSS policies.

e. Activities undertaken by NSA/CSS supporting the Defense Industrial Base Cybersecurity Program are subject to the DoD Chief Information Officer Memorandum (Reference j), including implementing guidance or agreements for the protection of USP information (USPI) consistent with DoDM 5240.01 (Reference c).

f. Cybersecurity activities undertaken by NSA/CSS fulfilling the responsibilities of the National Manager are not governed by DoDM 5240.01 (Reference c) but are subject to the Privacy Act (Reference m) and other applicable laws, regulations, or policies. However, it should be noted that DoDM 5240.01 (Reference c) governs any instance when mission activities involve the use of funds appropriated for intelligence activities, including any instance when *cybersecurity information* is made accessible for NSA/CSS intelligence analysis, use, etc. conducted pursuant to E.O. 12333 (Reference b).

g. All capabilities activities (e.g., processing data, developing analytics, fielding systems) undertaken by NSA/CSS that use operations information are governed by the approved procedures that are applicable to any information used to support the capabilities as enumerated in paragraphs 5.a–d.

h. All activities supporting foreign cryptologic partnerships—for either the SIGINT or the cybersecurity mission—undertaken by NSA/CSS or the USSS that use operations information are governed by the approved procedures applicable to the information under the partnership as enumerated in paragraphs 5.a–d.

i. All research activities undertaken by NSA/CSS that use operations information are governed by the approved procedures applicable to the information used to support the research as enumerated in paragraphs 5.a–d.

6. Before beginning any activity that may involve human subject research, approval must be obtained from the NSA/CSS HRPP (Human Research Protection Program) ("go HSR") in accordance with DoDI 3216.02, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Conducted and -Supported Research" (Reference o), and NSA/CSS Policy 10-10, "Protecting Human Subjects of Research" (Reference p). The subjects' informed *consent* shall be documented as required by DoDI 3216.02 and NSA/CSS Policy 10-10 (References o and p).

7. *Business information* containing USPI that supports the SIGINT and cybersecurity missions and authorized functions of NSA/CSS, including research, development, and other supporting and enabling mission activities, may be collected for *administrative purposes* pursuant to Procedure 2 of DoDM 5240.01 (Reference c). NSA/CSS may generate business information (i.e., information that is not derived from mission collection) to support its mission activities. All of this business information is not subject to the collection, query, retention, or dissemination requirements in Procedures 2 through 4 of DoDM 5240.01 (Reference c) but may be subject to other laws, E.O.s, or NSA/CSS policies.

8. NSA/CSS employees and members of the USSS must ensure that any USPI acquired with consent (either from a person or an organization)—to support a SIGINT or cybersecurity mission activity or for research functions—is appropriate for the purposes for which it is collected. The consent agreement, if required, must be express and documented in written or electronic form (e.g., consent form, template, email, terms of service, user agreement), unless exigent circumstances exist and a written or electronic consent is not feasible, in which case consultation with the NSA OGC (D2) is required before initiating collection. All consent agreements must be approved by the appropriate NSA/CSS official before targeting, collection, or querying can occur. Official consent form templates, staffing documents, and additional guidance related to individual consents may be found at "go consensual."

RESPONSIBILITIES

NSA Office of General Counsel (OGC, D2)

9. The NSA OGC (D2) shall:

a. In coordination with the Chief of Compliance (P7) and in consideration of the NSA Inspector General's (IG, I) independent oversight activities, conduct appropriate oversight to prevent or detect violations of DoDD 5240.01 (Reference a), E.O. 12333 (Reference b), this policy, and related laws, constitutional rights, E.O.s, directives, and regulations;

b. In coordination with the Chief of Compliance and the Director, Civil Liberties, Privacy, and Transparency (CLPT, D5), review and assess reports of activities that they have reason to believe may be unlawful or contrary to E.O.s or Presidential directives and of other *questionable intelligence activities (QIAs)* or *significant or highly sensitive matters (S/HSMs)* and provide other reports or information that the Intelligence Oversight Board (IOB) of the President's Intelligence Advisory Board or the DoD Senior Intelligence Oversight Official (DoD SIOO) requires;

c. Provide legal advice and assistance to all NSA/CSS employees and USSS elements regarding the mission activities covered by this policy;

d. Cooperate with NSA/CSS IG oversight of mission activities;

e. Assist the Chief of Compliance with development and execution of the NSA/CSS Comprehensive Mission Compliance Program;

f. Advise appropriate NSA/CSS organizations of new legislation and case law that may have an impact on NSA/CSS missions, functions, operations, activities, or practices;

g. Prepare any proposed changes to existing procedures or new procedures required by E.O 12333 (Reference b), FISA (Reference g), or any other legal authorities;

h. Prepare and process applications for authority to conduct collection pursuant to FISA (Reference g); and

i. Process requests from any Defense Intelligence Component, including NSA/CSS, for authority to use signals as described in DoDM 5240.01 (Reference c), paragraph 3.5.i.(1), "Developing, Testing, and Calibrating Electronic Equipment," for periods in excess of 90 days in the development, test, or calibration of electronic equipment that can intercept communications and other electronic surveillance equipment. Forward processed requests to the AG for approval when required.

Director, Civil Liberties, Privacy, and Transparency (CLPT, D5)

10. The Director, CLPT (D5) shall:

a. Serve as the senior official responsible for the protection of civil liberties and privacy in accordance with NSA/CSS Policy 12-1, "NSA/CSS Civil Liberties and Privacy Program" (Reference q);

b. Advise NSA/CSS senior leaders and mission managers regarding the protection of civil liberties and privacy, including reviewing new and novel uses of existing authorities and providing guidance related to AG-approved USP privacy procedures and FISA procedures in accordance with section 2000ee-1 of title 42 of the United States Code, "Privacy and Civil Liberties Officers" (Reference r), and DoDM 5240.01 (Reference c); and

c. In coordination with the NSA OGC (D2) and Compliance (P7), review and assess QIAs and S/HSMs and coordinate with the NSA/CSS Intelligence Oversight Officer (IOO) on its reports to the DoD SIOO. Reviews shall consider civil liberties and privacy impact even if the mission activity has been deemed to be compliant.

NSA/CSS Intelligence Oversight Officer (NSA/CSS IOO)

11. The NSA/CSS IOO shall:

a. Assist DIRNSA/CHCSS with conducting intelligence oversight in accordance with DoDD 5148.13, "Intelligence Oversight" (Reference s);

b. Establish a process for reporting mission compliance *incidents*, QIAs, or S/HSMs, which shall include engaging with CLPT (D5) for the assessment of civil liberty issues and, in partnership with the OGC (D2), coordinating their reporting externally to the DoD SIOO; and

c. Report annually to the DoD SIOO on behalf of DIRNSA/CHCSS on special circumstances collection in accordance with NSA/CSS Policy Memorandum 2021-01, "Special Circumstances: Guidance for Intelligence Collection of U.S. Person Information" (Reference u), and DoDM 5240.01 (Reference c) on approved special circumstances collection activities.

Chief of Compliance (P7)

12. The Chief of Compliance (P7) shall:

a. Serve as the Agency focal point and authority for programs of compliance over NSA/CSS mission activities and as the IOO in accordance with NSA/CSS Policy 12-2, "NSA/CSS Mission Compliance and Intelligence Oversight" (Reference t);

b. Coordinate with the National Cryptologic School (A2) to develop annual compliance training for all NSA/CSS employees and members of the USSS with mission requirements and access to operations information and operations data;

c. Establish incident reporting procedures to be followed by *directors*, extended Enterprise commanders/chiefs, and NSA/CSS representatives regarding their activities and practices as they relate to the Agency's assigned mission activities; and

d. In coordination with the NSA OGC (D2) and CLPT (D5), forward to the IOB of the President's Intelligence Advisory Board—through the DoD SIOO—reports of activities that they have reason to believe may be unlawful or contrary to E.O.s or Presidential directives and of other QIAs or S/HSMs and provide other reports or information that the IOB or the DoD SIOO requires.

NSA/CSS Inspector General (IG, I)

13. The NSA/CSS IG (I) shall, consistent with the Inspector General Act of 1978, as amended (Reference v), conduct appropriate oversight and inspections of NSA/CSS mission activities to prevent or detect violations of DoDD 5240.01 (Reference a), E.O. 12333 (Reference b), this policy, and related laws, constitutional rights, E.O.s, directives, and regulations.

Directors, NSA/CSS Chief of Staff, Extended Enterprise Commanders/Chiefs

14. Directors, the NSA/CSS Chief of Staff, and extended Enterprise commanders/chiefs shall:

a. Recognize, understand, and execute NSA/CSS cryptologic authorities in a compliant manner; manage, monitor, and perform mission activities in a manner consistent with the provisions of law and policy that are designed to protect civil liberties and privacy (Reference t);

b. Make training available to NSA/CSS employees and members of the USSS who have access to operations information regarding DoDD 5148.13 (Reference s), DoDM 5240.01 (Reference c), the SIGINT Annex (Reference d), and this policy on the requirements for collecting, processing, querying, retaining, and disseminating information;

c. Ensure that NSA/CSS employees involved in COMSEC monitoring are familiar with NSA/CSS Policy 3-1, "Information Assurance Monitoring" (Reference w);

d. Apply the provisions of this policy to all mission activities under their cognizance and ensure that all publications (e.g., U.S. SIGINT directives, national COMSEC instructions, NSA/CSS management and administrative publications) and instructions for which they are responsible are in compliance with this policy;

e. Conduct a periodic review of the mission activities and practices conducted in or under the cognizance of their respective organizations to ensure consistency with the laws and authorities listed in the references section of this policy;

f. Ensure that all new major requirements levied on NSA/CSS and the USSS or internally generated NSA/CSS requirements for mission activities are considered for review and approval by the NSA OGC (D2) and CLPT (D5) as required and comport with Compliance (P7) requirements and controls;

g. Ensure that the NSA OGC (D2) reviews mission activities that may raise a question of law or regulation before their acceptance or execution;

h. Ensure that necessary special security clearances and access authorizations are provided to the NSA OGC (D2), the IG (I), CLPT (D5), and the Chief of Compliance (P7) in order to enable them to meet their assigned responsibilities; and

i. Report as required in this policy and otherwise assist the NSA/CSS IOO and NSA OGC (D2) with carrying out their responsibilities.

NSA/CSS Employees and Members of the United States Signals Intelligence System (USSS):

15. NSA/CSS employees and members of the USSS shall:

a. Comply with the procedures outlined in DoDM 5240.01 (Reference c) and, when applicable, its classified SIGINT Annex (Reference d);

b. Complete all required compliance training and ensure that all required documentation (e.g., precondition agreements for memorandums of understanding/ memorandums of agreement) is approved before data access is granted; and

c. Report incidents, QIAs, and/or S/HSMs in accordance with NSA/CSS Policy 12-2 (Reference t).

REFERENCES

a. DoDD 5240.01, "DoD Intelligence Activities," dated 27 August 2014

b. E.O. 12333, "United States Intelligence Activities," dated 4 December 1981, and as amended

c. DoDM 5240.0l, "Procedures Governing the Conduct of DoD Intelligence Activities," dated 8 August 2016

d. DoDM S-5240.01-A, "Procedures Governing the Conduct of DoD Intelligence Activities: Annex Governing Signals Intelligence Information and Data Collected Pursuant to Section 1.7(c) of E.O. 12333," dated 7 January 2021

e. NSD 42, "National Policy for the Security of National Security Telecommunications and Information Systems," dated 5 July 1990

f. DoDD 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," dated 26 January 2010

g. "Foreign Intelligence Surveillance Act of 1978," as amended (50 United States Code 1801 et seq.)

h. E.O. 13587, "Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," dated 7 October 2011

i. DoDI 8500.01, "Cybersecurity," dated 14 March 2014

j. DoD Chief Information Officer Memorandum, "NSA Support to the Defense Industrial Base Cybersecurity Program," dated 4 May 2020

k. DoDI 8560.01, "Communications Security (COMSEC) Monitoring," dated 22 August 2018

l. Intelligence Community Directive 107, "Civil Liberties, Privacy, and Transparency," dated 28 February 2018

m. Privacy Act of 1974, as amended (5 United States Code 552a)

n. The National Telecommunications and Information Systems Security Directive No. 600, "Communications Security (COMSEC) Monitoring," dated 10 April 1990

o. DoDI 3216.02, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Conducted and -Supported Research," dated 15 April 2020

p. NSA/CSS Policy 10-10, "Protecting Human Subjects of Research," dated 18 June 2020

q. NSA/CSS Policy 12-1, "NSA/CSS Civil Liberties and Privacy Program," dated 18 November 2021

r. Section 2000ee-1, title 42, United States Code, "Privacy and Civil Liberties Officers," as amended, dated 19 January 2018

s. DoDD 5148.13, "Intelligence Oversight," dated 26 April 2017

t. NSA/CSS Policy 12-2, "NSA/CSS Mission Compliance and Intelligence Oversight," dated 1 March 2021

u. NSA/CSS Policy Memorandum 2021-01, "Special Circumstances: Guidance for Intelligence Collection of U.S. Person Information," dated 10 March 2021

v. Inspector General Act of 1978, as amended

w. NSA/CSS Policy 3-1, "Information Assurance Monitoring," dated 30 October 2020

GLOSSARY

administrative purposes—Information acquired for administrative purposes is information that is received or collected when it is necessary for the administration of NSA/CSS but is not received or collected directly for intelligence purposes. Examples include information about systems administration; the performance of contractors; public affairs and legislative matters, including correspondence files; personnel and training records; and training materials. (Reference c)

business information—Under NSA/CSS's authorities to collect, process, analyze, produce, and retain business information, the term "business information" here refers to business-related data/information about people, places, things, rules, events, or concepts used to operate and manage its Enterprise within the confines of its platform boundaries, including such internal administration or management information as network, personnel, medical, administrative, budget, or security records. (Source: NSA/CSS Policy Glossary)

consent—An agreement by a person or organization to permit NSA/CSS to take particular actions affecting that person or organization constitutes consent. Consent should be in written or in electronic form, but may be given orally, unless a specific form of consent is required by law or a particular procedure.

Consent may be implied if adequate notice is provided that a particular action carries with it the presumption of consent to an accompanying action. Consent may also be implied where adequate policy has been published or otherwise articulated.

The NSA General Counsel will determine whether a notice or policy is adequate and lawful before NSA/CSS takes or refrains from taking action on the basis of implied consent. (Reference c)

cooperating sources—Persons or organizations who knowingly or voluntarily provide information, or access to information, at the request of NSA/CSS, or on their own initiative are cooperating sources. These sources include government agencies, law enforcement authorities, credit agencies, commercial entities, academic institutions, employers, and foreign governments. (Reference c)

cryptologic—related to the collection and/or exploitation of foreign communications and non-communications emitters, known as signals intelligence, and solutions, products, and services to ensure the availability, integrity, authentication, confidentiality, and nonrepudiation of national security telecommunications and information systems, known as cybersecurity (Source: NSA/CSS Policy Glossary)

cybersecurity—prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (Source: NSA/CSS Policy Glossary)

cybersecurity information—A subset of operations information, cybersecurity information includes cybersecurity data and is acquired from monitoring, assessing, or analyzing national security systems and Department of Defense information systems for the purposes of defending networks, assessing threats, mitigating risk, and providing cryptographic solutions.

directors—the directors of Workforce Support Activities (A), Business Management and Acquisition (B), Cybersecurity (C), Engagement and Policy (P), Research (R), Operations (X), and Capabilities (Y) (Source: NSA/CSS Policy Glossary)

electronic surveillance—This collection technique is the acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter. Electronic surveillance is also defined in FISA (the Foreign Intelligence Surveillance Act of 1978) (Reference g), and where these procedures reference that definition, FISA should be consulted. (Reference c)

incident—any NSA/CSS mission or mission-related activity that may deviate from laws, Executive orders, and policies governing signals intelligence and/or cybersecurity mission activities and that must be reported immediately upon recognition using the Agency-approved incident management tool ("go IRT") (Source: NSA/CSS Policy Glossary)

information supporting cryptologic operations (ISCO)—A subset of operations information and operations data, ISCO is acquired under NSA/CSS authorities (e.g., Executive Order 12333, National Security Directive 42), and is publicly available, provided from cooperating sources (i.e., commercially acquired or voluntarily provided to NSA/CSS) or collected through any other techniques authorized pursuant to NSA/CSS authorities, excluding electronic surveillance and monitoring of national security systems and Department of Defense systems. This definition excludes signals intelligence (SIGINT) information (including consensual SIGINT collection) and cybersecurity information.

NSA/CSS employee—a person employed by, assigned or detailed to, or who otherwise conducts authorized mission activities on behalf of NSA/CSS or in fulfillment of the responsibilities of the

National Manager for National Security Systems (Derived from Reference c, General Provisions section and definition of Defense Intelligence Component employee)

NSA/CSS mission and mission-related activities—activities conducted under the authority, direction, or control of the Director, NSA/Chief, CSS, including signals intelligence and/or cybersecurity operations and all activities needed to support those mission areas (Source: NSA/CSS Policy Glossary)

operations data—Under NSA/CSS's authorities to collect, process, analyze, produce, retain, and disseminate, operations data refers to the individual numbers, characters, images, or other method of recording, in a form suitable for communication, interpretation, or processing, which can be assessed by a human or entered into a computer, stored or processed on a computer, or transmitted on some digital channel. Operations data is provided to, or acquired, generated, or otherwise collected by, NSA/CSS organizations under NSA/CSS authorities for cryptologic mission and related purposes, including information for research, development, test, mission management, and training purposes. (Source: NSA/CSS Policy Glossary)

operations information—Under NSA/CSS's authorities to collect, process, analyze, produce, retain, and disseminate, operations information refers to cryptologic and cryptologic-related information, including foreign intelligence and counterintelligence. This definition also includes operations data or information acquired or collected in order to protect and defend national security systems and Department of Defense networks. Operations information implies interpretation of operations data to produce facts and other products and services. Operations information implies interpretation of operations data to produce facts and other products and services includes SIGINT (signals intelligence) information, cybersecurity information, and information supporting cryptologic operations. Operations information does not include such internal administration or management information as personnel, medical, administrative, budget, or security records. (Source: NSA/CSS Policy Glossary)

questionable intelligence activity (QIA)—any intelligence or intelligence-related activities in which there is a reason to believe that such activity may be unlawful or contrary to an Executive order, Presidential directive, Intelligence Community directive, or applicable Department of Defense policy governing that activity (Source: NSA/CSS Policy Glossary)

signals intelligence (SIGINT)—a category of intelligence comprising, either individually or in combination, all COMINT (communications intelligence), ELINT (electronic intelligence), and FISINT (foreign instrumentation signals intelligence), however transmitted (Source: DoDI O-3115.07, "Signals Intelligence," dated 15 September 2008)

signals intelligence (SIGINT) information—A subset of operations information, SIGINT information, which includes SIGINT data, is acquired by electronic surveillance.

significant or highly sensitive matter (S/HSM)—An S/HSM is an intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an Executive order, Presidential directive, Intelligence Community (IC) directive,

or Department of Defense policy), or serious criminal activity by intelligence personnel that could impugn the reputation or integrity of the IC, or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential congressional inquiries or investigations; adverse media coverage; impact on foreign relations or foreign partners; and systemic compromise, loss, or unauthorized disclosure of protected information. (Source: NSA/CSS Policy Glossary)

United States Signals Intelligence System (USSS)—The organization unified under the DIRNSA/CHCSS's authority to conduct signals intelligence (SIGINT), the USSS includes NSA and components of the military services (including the U.S. Coast Guard) that are authorized to conduct SIGINT activities and such other entities authorized by the Secretary of Defense or the Director, NSA to conduct SIGINT activities pursuant to section 1.7(c)(2) of Executive Order 12333. The USSS does not include foreign cryptologic partners. A Department of Defense component is not to be considered part of the USSS with respect to its non-SIGINT activities, and such activities are not governed by the SIGINT Annex. (Reference d)

U.S. person (USP)—includes:

a. A U.S. citizen;

b. An alien known by the NSA/CSS to be a permanent resident alien;

c. An unincorporated association substantially composed of U.S. citizens or permanent resident aliens;

d. A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a U.S. person;

e. A person or organization in the United States is presumed to be a USP unless specific information to the contrary is obtained. Conversely, a person or organization outside the United States or whose location is not known to be in the United States is presumed to be a non-USP, unless specific information to the contrary is obtained. (Reference c)

DOCUMENT HISTORY

Date	Approved by	Description
10 January 2022	Paul M. Nakasone, General, U.S. Army; Director, NSA/Chief, CSS	Policy reissuance; supersedes NSA/CSS Policy 1-23, "Procedures Governing NSA/CSS Activities That Affect U.S. Persons," dated 27 August 2020, and NSA/CSS Policy Memorandum 2018-02, "Guidance for NSA/CSS Non-Intelligence

Date	Approved by	Description
		Activities That Affect U.S. Persons," dated 15 March 2021
15 February 2022	Chief, Policy	Administrative update to change organization name from ATSD (PCLT) to DoD SIOO, to edit paragraph 3.a, and to revise control markings