NSA/CSS POLICY 12-2
NSA/CSS MISSION COMPLIANCE AND INTELLIGENCE OVERSIGHT

DATE:	30 July 2021 (See Document History.)
OFFICE OF PRIMARY INTEREST:	Compliance Group (P7), 963-8500 (secure)
RELEASABILITY:	NSA/CSS Policy 12-2 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:	1 March 2021

PURPOSE AND SCOPE

1. In accordance with the National Security Agency Act of 1959 and Department of Defense Directive (DoDD) 5148.13, "Intelligence Oversight" (References a and b), this policy establishes the requirements for intelligence *oversight* and assigns responsibilities related to the NSA/CSS *Comprehensive Mission Compliance Program (CMCP)*.

2. This policy applies to all *personnel* conducting *NSA/CSS mission and mission-related activities* (hereafter referred to as "mission activities") in support of producing *signals intelligence (SIGINT)* and/or *cybersecurity* products and services under the authority, direction, or control of the Director, NSA/Chief, CSS (DIRNSA/CHCSS) or using data acquired under the mission authority of NSA/CSS (References a–cc).

POLICY

3. NSA/CSS shall execute its missions of protecting U.S. national security systems and producing SIGINT information in a lawful manner (References a–cc). NSA/CSS is also fully committed to protecting privacy and civil liberties during the conduct of its mission activities (Reference c).

4. The NSA/CSS CMCP shall provide reasonable assurance that SIGINT and/or cybersecurity missions, as well as other mission activities in which NSA/CSS mission data is employed, are conducted in a manner that is consistent with the requirements contained in References a–cc and that protects privacy and civil liberties. The development and implementation of the CMCP supports the NSA/CSS civil liberties and privacy program.

5. DIRNSA/CHCSS shall appoint an *NSA/CSS Intelligence Oversight Officer (IOO)* to develop and administer an intelligence oversight *compliance* program that is tailored to the

Agency's SIGINT and/or cybersecurity mission requirements. The IOO shall develop intelligence oversight implementation guidance and conduct periodic reviews of mission activities to verify compliance with federal law, Executive orders, Presidential directives, Intelligence Community directives, and DoD and NSA/CSS policy (Reference b).

6. *Mission owners/elements* (hereafter referred to as "mission owners")—including field leaders, *extended Enterprise* leaders, and Service cryptologic component commanders, directors, and commandants—shall know, understand, and execute the authorities granted to NSA/CSS to conduct mission in a manner that complies with the rules that protect privacy (References a–cc).

7. NSA/CSS organizations shall report, investigate, and mitigate potential mission compliance *incidents*, *questionable intelligence activities (QIAs)*, and/or *significant or highly sensitive matters (S/HSMs)* upon recognition and in accordance with this policy, and shall take appropriate corrective actions as needed (References b and d–n).

8. All personnel shall report potential mission compliance incidents, QIAs, and/or S/HSMs immediately upon recognition using the Agency-approved incident management tool ("go IRT") or in accordance with compliance guidance ("go incident reporting") (References a, b, and d–f).

9. Nothing in this issuance shall be construed as impinging upon the authorities or independence of the Inspector General of the DoD, the Inspector General of NSA/CSS (I), or any other statutory inspector general, as provided by the Inspector General Act of 1978 (Reference o).

PROCEDURES

10. The CMCP consists of all mission compliance and intelligence oversight activities performed to protect privacy while conducting NSA/CSS SIGINT and/or cybersecurity missions ("go compliance"). Accordingly, in implementing the CMCP, the Compliance Group (P7) will:

a. Develop compliance controls throughout NSA/CSS workflows and architecture to support efficient and compliant operations;

b. Manage the NSA/CSS Mission System Compliance Certification Process to confirm that mission systems are developed and operated in accordance with applicable laws and policies;

c. Verify that mission systems are functioning and mission activities are being performed in a compliant manner;

d. Issue appropriate and timely rules, regulations, and guidance as needed;

e. Develop and provide compliance training;

f. Raise awareness of compliance processes and procedures;

g. Provide compliance support to mission activity operations;

h. Serve as the authoritative lead of the Analytics Vetting Group (AVG) ("go AVG"), which oversees the *Analytic Management Process* ("go AVP") and controls the life cycle of mission *analytics* to ensure equitable deployment and compliant control of affiliated systems (Reference p);

i. Manage the transition and decommissioning of legacy mission systems to provide reasonable assurance of compliance with applicable laws and policies ();

j. Support ongoing research to improve the agility and efficiency of the CMCP;

k. Conduct compliance *risk assessments* in accordance with NSA/CSS Policy 1-71, "Enterprise Risk Management" (Reference q) and the procedures provided by the Compliance Group ("go compliance") in order to offer reasonable assurance that the CMCP is informed by identified risks within the mission activity process; and

l. Provide personnel with the Agency-approved incident management tool ("go IRT") to report potential mission compliance incidents, QIAs, and/or S/HSMs immediately upon recognition (for additional information, "go incident reporting").

11. New and updated mission compliance and intelligence oversight guidance will be published on the Compliance Group (P7) web page ("go compliance").

RESPONSIBILITIES

Director, NSA/Chief, CSS (DIRNSA/CHCSS)

12. DIRNSA/CHCSS shall:

a. Appoint a Director of Compliance who shall be responsible for the CMCP for all mission activities under the authority of NSA/CSS (Reference r); and

b. Appoint an NSA/CSS IOO who is authorized to administer an intelligence oversight program tailored to NSA/CSS mission activities (i.e., the CMCP) and issue intelligence oversight compliance guidance in support of this program (Reference b).

NSA/CSS Intelligence Oversight Officer (IOO)

13. The NSA/CSS IOO shall:

a. Assist DIRNSA/CHCSS in conducting intelligence oversight in accordance with DoDD 5148.13 (Reference b);

b. Develop and implement authoritative intelligence oversight and mission compliance guidance for NSA/CSS mission activities and conduct periodic reviews of mission activities to provide reasonable assurance that these activities are conducted in a manner consistent with applicable laws, Executive orders, regulations, directives, policies, and formal agreements (References a–f, h–k, n, and r);

c. Establish a process for reporting potential mission compliance incidents, QIAs, or S/HSMs, which will include engaging with the Office of Civil Liberties, Privacy, and Transparency (CLPT, D5) for the assessment of civil liberty issues and, in partnership with the Office of General Counsel (OGC, D2), coordinating their reporting externally to the DoD Senior Intelligence Oversight Official (SIOO);

d. Administer an intelligence oversight training program that is tailored to NSA/CSS mission activity requirements and includes:

1) Identifying the authorities and restrictions governing applicable intelligence activities (References a–cc);

2) Outlining the responsibilities of DoD personnel and DoD contractor personnel for reporting potential mission compliance incidents, QIAs, and S/HSMs (Reference b); and

3) Providing initial and annual refresher intelligence oversight and intelligence-related activities training to mission personnel; and

e. Acquire access to all NSA/CSS mission activity, intelligence, and intelligence-related activity as needed, in order to allow those protected by special-access programs, alternative compensatory control measures, and other security compartments to report on intelligence oversight and mission compliance (Reference b).

Chief, Compliance Group (P7)

14. The Chief, Compliance Group (P7) shall:

a. Serve as the Director of Compliance (Reference r);

b. Serve as the NSA/CSS IOO (Reference b);

c. Advise DIRNSA/CHCSS and NSA/CSS leaders on the compliant execution of NSA/CSS mission activities;

d. Develop and implement comprehensive mission compliance and intelligence oversight training in conjunction with OGC (D2), the National Cryptologic School (NCS, A2), and appropriate NSA/CSS stakeholders, as applicable (References a–f, j, k, r, and s);

e. Establish, implement, and monitor the CMCP to assist NSA/CSS in effectively carrying out its responsibility to protect privacy during the conduct of NSA/CSS mission activities by:

1) Improving NSA/CSS's compliance posture through the development and implementation of intelligence oversight and mission compliance-related guidance (e.g., compliance directives), policies, training, customer engagements, communications, and events (References b and d);

2) Continually developing, implementing, and, when practicable, automating controls, processes, policies, and systems to advance NSA/CSS's compliance posture;

3) Delivering tailored intelligence oversight and mission compliance support as appropriate to NSA/CSS's mission owners and throughout the extended Enterprise by engaging *compliance officers* and *oversight officers*;

4) Assessing the effectiveness of the CMCP by monitoring and verifying (References d and r) that mission activities are conducted in compliance with applicable laws, Executive orders, policies, and regulations (References a–cc);

5) Participating in mission compliance risk assessments, Enterprise risk assessments, and compliance reviews to identify and mitigate areas of potential mission non-compliance and to help guide mission activities;

6) Providing subject matter expertise and guidance as needed to parties developing and implementing compliance programs that will inform access to and usage and handling of NSA/CSS equities, particularly when such programs and/or equities address privacy protections, including—without limitation—the proper handling and protection of SIGINT, SIGINT-derived, and/or cybersecurity data used by partner elements (including academic and commercial entities, U.S. Government elements, and *Second Party* and *Third Party* partners);

7) Partnering with mission owners and other organizations to take appropriate corrective actions as needed to provide reasonable assurance of compliant conduct for NSA/CSS mission activities;

8) Issuing compliance directives that define and establish guidance for mission owners concerning oversight officer operational activities and responsibilities and that inform the compliance officer work role and responsibilities; and

9) Advocating, advising, and overseeing innovation, research, and experimentation that seek to close mission compliance capability gaps and advance NSA/CSS's compliance posture;

f. Partner with Capabilities (Y) to build compliance controls into mission systems, including, without limitation:

1) Developing and supporting capabilities used for SIGINT and/or cybersecurity mission activity purposes that help implement the requirements contained in References a–cc, as applicable;

2) Coordinating with the NSA/CSS Chief Data Officer on the compliant management of NSA/CSS's mission data governance processes, including business rules and cryptologic data tagging, in order to enable the appropriate

execution of compliance functions and the implementation of critical compliance controls;

3) Monitoring, verifying, and assessing the technical compliance health of mission systems and analytics;

4) Establishing and prescribing mission system certification requirements and data management processes to support privacy and other legal obligations;

5) Coordinating and advocating for integration of consistent technical compliance capabilities across the NSA/CSS infrastructure (Reference p) and the Intelligence Community Information Technology Enterprise architectures; and

6) Serving as the authoritative lead of the AVG per the AVG Charter;

g. Manage the NSA/CSS Mission System Compliance Certification Process by reviewing and issuing compliance certification of NSA/CSS systems for legal and policy compliance concerning privacy protections;

h. Monitor and verify NSA/CSS mission compliance by:

1) Managing the reporting and tracking of potential non-compliant mission activities, QIAs, and/or S/HSMs to be reported in accordance with DoDD 5148.13 and facilitating non-compliant incident mitigation with appropriate organizations (Reference b);

2) Partnering with mission owners to ensure that potential mission compliance incidents, QIAs, and S/HSMs are reported immediately upon recognition in the Agency-approved incident management tool ("go IRT"), regardless of mission authority (Reference b);

3) Partnering with OGC (D2) to review and substantiate QIAs and S/HSMs; and

4) Producing metrics and incident trends, conducting root cause analysis, and performing verification activities in order to provide reasonable assurance of compliance with the rules designed to protect privacy (References a–i and r–v);

i. Engage with external and internal organizations regarding compliance by:

1) (U) Participating in and, as appropriate, leading NSA/CSS's engagement with external organizations that conduct oversight of NSA/CSS mission activities, in concert with OGC (D2), CLPT (D5), Legislative, State and Local Affairs (P3), Authorities Integration, and other NSA/CSS organizations, as appropriate (Reference h);

2) Planning and leading routine interactions with external organizations, including periodic oversight reviews of NSA/CSS's operations under the Foreign Intelligence Surveillance Act with overseers from the Department of Justice (Reference h);

3) Validating the effective incorporation of compliance controls and safeguards within written support agreements for customers and partners in order to provide reasonable assurance of compliant mission activities; and

4) Assisting with developing and implementing compliance programs for academic and commercial communities, U.S. Government elements, and partners when they are operating under the direction, authority, control, or delegated authority of DIRNSA/CHCSS;

j. Partner with mission owners when they engage with external overseers regarding compliance of mission-related activities;

k. Partner with mission owners to establish measures to protect privacy and limit access to and use of such information to those employees who have the appropriate security clearances, mission data accesses, appropriate training, and an approved, documented mission requirement through the Agency mission entitlement system (References l, m, r, w, and x);

l. Respond to requests from the DoD Component legal counsel, the DoD General Counsel, the DoD SIOO, and any inspector general of competent jurisdiction in accordance with NSA/CSS policy; and

m. Partner with Capabilities (Y), mission owners, OGC (D2), and, as needed, CLPT (D5), to provide reasonable assurance of compliance with all laws and policies during the transition and decommissioning of NSA/CSS mission systems, enabling the orderly shutdown of legacy systems by:

1) Conducting careful analyses to minimize mission activity impact and provide reasonable assurance of compliance with all applicable laws, policies, directives, and procedures; and

2) Ensuring that all facets of compliant operations are considered for both the legacy system and the other products and services receiving the legacy functions.

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

15. CLPT Office (D5) shall:

a. Review and assess QIAs and S/HSMs provided by the Compliance Group (P7) for issues related to privacy and civil liberties concerns;

b. Recommend internal controls or other safeguards for civil liberties and privacy as integral parts of the CMCP;

c. Partner with OGC (D2) and the Compliance Group to review QIAs and coordinate with the NSA/CSS IOO on its reports to the DoD SIOO (Reference b) (reviews will consider civil liberties and privacy impact even if the mission activity was deemed to be compliant); and

d. As needed, partner with the Capabilities Directorate (Y), mission owners, OGC (D2), and the Compliance Group to transition operational mission functions to other products and services, enabling the orderly shutdown of legacy systems through careful analysis to minimize mission activity impact and provide reasonable assurance of compliance with all applicable laws, policies, directives, and procedures.

Capabilities Directorate (Y)

16. The Capabilities Directorate (Y) shall:

a. Develop and support capabilities used across the NSA/CSS Enterprise and for external organizations for SIGINT and/or cybersecurity mission activities (References a–cc, as applicable);

b. Partner with the Compliance Group (P7) and mission owners to build compliance controls into mission systems, including, without limitation:

1) Developing and supporting capabilities used for SIGINT and/or cybersecurity mission activity purposes that comply with the requirements contained in References a–cc, as applicable;

2) Coordinating with the NSA/CSS Chief Data Officer on the compliant management of NSA/CSS's mission data governance processes, including business rules and cryptologic data tagging, in order to enable the appropriate execution of compliance functions and the implementation of critical compliance controls;

3) Monitoring, verifying, and assessing the technical compliance health of mission systems and analytics;

4) Assisting in the development of mission system compliance certification requirements and data management processes to support privacy and legal obligations; and

5) Coordinating and advocating for the integration of consistent technical compliance capabilities across the NSA/CSS infrastructure (Reference p) and the Intelligence Community Information Technology Enterprise architectures;

c. Support the Compliance Group in monitoring, verifying, and assessing the technical compliance health of mission systems and analytics;

d. Require that mission systems satisfy the mission system compliance certification requirements and undergo the System Certification Process;

e. Coordinate and advocate for the integration of consistent technical compliance capabilities across the NSA/CSS infrastructure and the Intelligence Community Information Technology Enterprise architectures;

f. Participate in the AVG;

g. Support the Compliance Group with conducting technical reviews of mission systems and analytics to help ensure the effective incorporation and functioning of compliance requirements, safeguards, and standards, in order to provide reasonable assurance that they are compliant with legal and policy obligations; and

h. Partner with mission owners, OGC (D2), the Compliance Group (P7), and, as needed, CLPT (D5), to transition operational mission functions to other products and services, enabling the orderly shutdown of legacy systems through careful analysis to minimize mission activity impact and provide reasonable assurance of compliance with all applicable laws, policies, directives, and procedures.

Office of the General Counsel (OGC, D2)

17. OGC (D2) shall:

a. Provide legal advice on matters relating to mission activities to guide NSA/CSS in conducting them in compliance with the rules designed to protect privacy;

b. Act as lead interlocutor for and coordinator of all non-routine NSA/CSS compliance-related engagements with the Department of Justice, the Foreign Intelligence Surveillance Court, and other key external legal stakeholders, as warranted;

c. Partner with the Compliance Group (P7) to review and substantiate potential mission compliance incidents, QIAs, and S/HSMs, and coordinate with the NSA/CSS IOO to report notices of S/HSMs to the DoD SIOO (Reference b);

d. Partner with the Compliance Group (P7), NCS (A2), and the appropriate NSA/CSS stakeholders to develop and update mission compliance and intelligence oversight training; and

e. Partner with Capabilities (Y), mission owners, the Compliance Group (P7), and, as needed, CLPT (D5), during the transition and decommissioning of NSA/CSS legacy mission systems, enabling the orderly shutdown of legacy systems through careful

analysis to minimize mission activity impact and provide reasonable assurance of compliance with all applicable laws, policies, directives, and procedures.

National Cryptologic School (NCS, A2)

18. The NCS (A2) shall coordinate with the Compliance Group (P7), OGC (D2), and the appropriate NSA/CSS stakeholders to implement and update comprehensive mission compliance and intelligence oversight training (References a–f, r, and t).

Mission Owners

19. Mission owners shall:

a. Recognize, understand, and execute in a compliant manner the authorities granted to NSA/CSS for their cryptologic mission (Reference t);

b. Manage, monitor, and perform SIGINT and/or cybersecurity mission activities in a manner consistent with the provisions of law and policy that are designed to protect privacy (References a–cc);

c. Direct their organizational mission personnel to complete initial and refresher compliance training in a manner that is consistent with NSA/CSS requirements to ensure that mission personnel are fully informed of their responsibility to perform mission activities in a compliant manner;

d. Partner with the Compliance Group (P7) to fully integrate the NSA/CSS CMCP into their organizations' mission and maintain effective compliance programs and procedures in their organizations (References a, b, d–f, r, and y);

e. Coordinate with Capabilities (Y) and the Compliance Group (P7) to incorporate compliance controls in the development and support of capabilities used across the NSA/CSS Enterprise and for external organizations for SIGINT and/or cybersecurity mission activity (References a–cc, as applicable);

f. Evaluate mission activities for adherence to applicable laws, directives, and agreements, and collaborate with the Compliance Group and other NSA/CSS organizations to take appropriate corrective actions as needed to ensure compliant conduct of mission (References a–i and r–v);

g. Partner with the Compliance Group representatives to ensure that potential mission compliance incidents, QIAs, and/or S/HSMs are reported immediately upon recognition in the Agency-approved incident management tool ("go IRT") in accordance with compliance guidelines, regardless of mission authority (Reference b);

h. Partner with the Compliance Group when engaging with external overseers regarding compliance mission-related activities;

i. Partner with the Compliance Group to establish measures to protect privacy and limit access to use of information to those employees who have the appropriate security clearances, mission data accesses, appropriate training, and an approved, documented mission requirement through the Agency mission entitlement system (References e, f, l, m, w, and x);

j. Coordinate the documentation of all locations where authorized mission activities are being conducted in accordance with NSA/CSS's SIGINT Authorities Matrix and subsequent cybersecurity guidance;

k. Coordinate for approval and documentation, via NSA/CSS's Corporate Action Tracking System, all locations throughout the extended Enterprise where authorized mission activities are conducted—including delegated missions and missions worked at approved, alternate locations (e.g., hoteling and flexiplace)—and, upon approval, ensure that authorizations are uploaded within the Agency-approved mission entitlement system (Reference j);

l. Promote compliance with data management and storage requirements and take steps to ensure that any data copied or moved from any corporate data repository is handled in a manner consistent with all relevant authoritative practices and standards;

m. Assign at least two properly trained oversight officers per mission location within each *Mission Correlation Table* under the mission owner's purview (mission owners may delegate the authority to assign oversight officers and may request waivers related to the oversight officer requirement to the Chief, Compliance Group via the corporate SPF (Staff Processing Form) process);

n. Manage and monitor mission activities in accordance with applicable security and compliance requirements and provide appropriate resources, including post-query review (auditing) and tasking adjudication, which includes recognizing, understanding, and executing the authorities granted to NSA/CSS for their cryptologic mission; and

o. Partner with OGC (D2), the Compliance Group (P7), Capabilities (Y), and, as needed, CLPT (D5), during the transition and decommissioning of NSA/CSS legacy mission systems, enabling the orderly shutdown of legacy systems through careful analysis to minimize mission activity impact and provide reasonable assurance of compliance with all applicable laws, policies, directives, and procedures.

Compliance Officers

20. Compliance officers shall provide reasonable assurance of compliance with the requirements contained in References a–cc, as appropriate, by:

a. Following procedures and guidance issued by the Compliance Group (P7) in support of the strategic development, implementation, and monitoring of the NSA/CSS CMCP;

b. Participating in compliance risk assessments;

c. Developing compliance controls, requirements, standards, and procedures;

d. Supporting the development and promoting awareness of mission compliance and intelligence oversight training; and

e. Supporting the development of and promoting awareness of verification activities.

Oversight Officers

21. Oversight officers shall:

a. Understand and implement the authorities, mission activities, and relevant policies associated with the specific mission areas they support (Reference u);

b. Implement, manage, and provide daily compliance and intelligence oversight guidance to colleagues conducting mission activities; and

c. Follow procedures and guidance issued by the Compliance Group (P7) in support of the NSA/CSS CMCP.

All Personnel Who Conduct or Are Involved in NSA/CSS Mission Activities

22. All personnel who conduct or are involved in NSA/CSS mission activities shall:

a. Know, understand, and execute the authorities granted to NSA/CSS for mission purposes in compliance with the rules designed to protect privacy;

b. Exercise *due diligence* in conducting activities in compliance with rules designed to protect privacy and take measures to reduce the risk of non-compliant activity (References d–g, k–n, r, s, and u);

c. 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 (References b–g, k–n, r, s, u, and w);

d. Report any potential mission compliance incidents, QIAs, and/or S/HSMs immediately upon recognition to management, an oversight officer, and the Compliance Group (P7) using the Agency-approved incident management tool ("go IRT") (Reference b); and

e. Adhere to the statutory and policy rules for compliance with all data sets while working under DIRNSA/CHCSS's authority and ensure that any data emailed, copied, or moved from the corporate data repositories is handled in accordance with the statutory and policy rules associated with the data (e.g., retention rules, purge obligations, dissemination methodology).

REFERENCES

a. National Security Act of 1959, as amended through P.L. 113–126, enacted 7 July 2014

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

c. NSA/CSS Policy 1-34, "Implementation of the Privacy Act of 1974," dated 30 October 2020

d. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981 (as amended by Executive Orders 13284 (2003), 13355 (2004), and 13470 (2008)

e. DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," dated 8 August 2016

f. DoD Manual S-5240.01-A, "Signals Intelligence," dated 7 January 2021

g. NSA/CSS Policy 1-23, "Procedures Governing NSA/CSS Activities That Affect U.S. Persons," dated 27 August 2020

h. United States Signals Intelligence Directive (USSID) 19, "NSA/CSS Signals Intelligence Directorate—Oversight and Compliance Policy," revised 29 January 2014

i. Foreign Intelligence Surveillance Act (FISA), as amended, 10 July 2008

j. USSID SP0018, "Legal Compliance and U.S. Persons Minimization Procedures," dated 25 January 2011

k. USSID SP0018, "Supplemental Procedures for the Collection, Processing, Retention and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons," dated 12 January 2015

l. Signals Intelligence Directive 421, "United States SIGINT System Database Access," revised 9 June 2015

m. USSID CR1610, "SIGINT Production and Raw SIGINT Access," revised 9 March 2016

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

o. Inspector General Act of 1978, Public Law 95-452, §1, 12 October 1978

p. NSA/CSS Technology Directorate Management Directive 004, "Technology Directorate Compliance," dated 5 August 2016

q. NSA/CSS Policy 1-71, "Enterprise Risk Management," dated 27 August 2020

r. 2010 Intelligence Authorization Act (Public Law 111-259), dated 10 October 2010

s. DoD Regulation 5240.1-R, Change 2, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," dated 26 April 2017

t. NSA/CSS Policy 1-3, "NSA/CSS Governance," dated 2 March 2020

u. NSA/CSS Policy 11-10, "Dual Authorities Operations," dated 14 August 2020

v. National Telecommunications and Information Systems Security Directive 600, "Communications Security (COMSEC) Monitoring," dated 10 April 1990

w. NSA/CSS Policy Instruction 2-0002, dated 18 June 2020

x. Presidential Policy Directive-28, "Signals Intelligence Activities," dated 17 January 2014

y. NSA/CSS Policy 11-5, "Forensics," dated 20 December 2019

z. NSA/CSS Policy 7-3, "Managers' Internal Control Program," dated 13 September 2019

aa. NSCID 6, "Signals Intelligence," dated 17 February 1972

bb. NSA/CSS Policy 11-1, "Information Sharing," dated 30 October 2020

cc. NSA/CSS Policy 11-12, "NSA/CSS Support to the Defense Industrial Base Cybersecurity Program," dated 13 October 2020

(U) GLOSSARY

Analytic Management Process—The Analytic Management Process is NSA/CSS's authoritative process to manage the mission prioritization of analytics and provide a framework for their equitable deployment and control in meeting compliance, policy, and regulatory requirements.

analytics—"Analytics" refers to an automated process used to manipulate, combine, organize, measure, enrich, correlate, or learn from data. Analytics range from customized solutions supporting niche requirements to corporate solutions supporting varied missions and organizations at scale and may exist for a limited duration (hours/days/weeks) or be sustained for years as appropriate to mission needs.

compliance—verifiable conformance with a set of clearly defined rules/standards; in NSA/CSS mission, refers to compliance with the rules designed to protect privacy and civil liberties

compliance officers—employees authorized by the NSA/CSS Compliance Group (P7) to assist oversight officers and personnel with conducting mission activities in compliance with the requirements in NSA/CSS Policy 12-2.

Comprehensive Mission Compliance Program (CMCP)—The CMCP is a broad collection of activities and initiatives that direct the people, processes, systems, and resources needed to

achieve reasonable assurance that signals intelligence and/or cybersecurity missions are verifiably conducted in accordance with the laws and policies that afford privacy protection. The CMCP addresses the integration of compliance strategies and activities across NSA/CSS mission, technology, and policy organizations; a training and education program for compliance; and the maintenance of and reporting on the status of mission compliance at NSA/CSS, including performing trend analysis and providing well-reasoned corrective measures. (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 their availability, integrity, authentication, confidentiality, and nonrepudiation (Source: NSA/CSS Policy Glossary)

due diligence—exercise of reasonable care in ensuring that compliance measures have been implemented to protect privacy during all phases of mission activities

extended Enterprise—NSA/CSS personnel, systems, and facilities at locations other than NSA/Washington (Source: NSA/CSS Policy Glossary)

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")

Mission Correlation Table (MCT)—MCTs consist of the key information used by the Enterprise mission entitlement database to tie personnel to the entitlements needed for mission activity.. (Reference o)

mission owners/elements—Enterprise leaders, field leaders, extended Enterprise leaders, Service cryptologic component commanders, directors/commandants, and others who exercise Director, NSA/Chief, CSS–derived authority to enable, direct, manage, and/or conduct cryptologic activities and operations (signals intelligence and/or cybersecurity) in any NSA/CSS directorate

NSA/CSS Intelligence Oversight Officer (IOO)—The NSA/CSS IOO is a Director, NSA/Chief, CSS appointee authorized to develop and administer a tailored intelligence oversight and mission compliance program for NSA/CSS and to issue related intelligence oversight and mission compliance guidance and training in accordance with Department of Defense Directive 5148.13, "Intelligence Oversight" (Reference b). The position of NSA/CSS IOO differs from that of the mission oversight officer.

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

oversight—Oversight, for the purposes of this policy, is the independent inspection or review of signals intelligence and/or cybersecurity activities to verify that they are conducted in a manner consistent with the laws, regulations, and policies designed to protect privacy. External oversight is conducted primarily by independent entities (e.g., the Office of the Inspector General, congressional overseers, and Executive Branch oversight personnel) to ensure objectivity when assessing the performance of NSA/CSS compliance efforts. Internal NSA/CSS mission activity oversight is conducted primarily by oversight officers.

oversight officer—Oversight officers are individuals who are assigned by mission owners based on their subject matter expertise to conduct daily oversight of signals intelligence (SIGINT) and/or cybersecurity activities at a location where SIGINT and/or cybersecurity missions are conducted. Oversight officers advise local management and mission members of compliance risks and mitigations and must complete mandatory compliance and oversight training, as well as necessary training for their mission activities.

personnel—for purposes of this policy only, all affiliates employed by or conducting mission activities and related activities under the authority, direction, or control of the Director, NSA/Chief, CSS or where applicable, using data acquired under the authority of NSA, including all civilian and military employees, detailees, integrees, assignees, designees, contractors, and persons otherwise acting at the direction of NSA/CSS

questionable intelligence activity (QIA)—any intelligence or intelligence-related activity when there is 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 (Reference b)

risk assessment—A risk assessment is an interactive process for identifying and assessing risks that may limit the achievement of Enterprise objectives (e.g., compliant mission activities) using qualitative and quantitative factors. Risk assessments follow a basic risk analysis framework to assess and prioritize risks in a way that gives insight into the risk exposures from non-compliance with the rules to protect privacy and information.

Second Party—any of the four countries with which the U.S. Government maintains signals intelligence and/cybersecurity relationships, namely Australia, Canada, New Zealand, and the United Kingdom (Source: NSA/CSS Policy Glossary)

signals intelligence (SIGINT)—a category of intelligence comprising either individually or in combination, all communications intelligence, electronic intelligence, and foreign instrumentation intelligence, regardless of the mode of transmission and whether information is being transmitted at the time of acquisition

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 (Reference b).

Third Party—any country with which the U.S. Government maintains signals intelligence, and/or cybersecurity relationships other than Australia, Canada, New Zealand, and the United Kingdom (Source: NSA/CSS Policy Glossary)

U.S. person—a citizen of the United States; an alien lawfully admitted as a permanent resident in the United States (also known as a green card holder); an unincorporated group or association whose members are substantially either citizens of the United States or aliens lawfully admitted for permanent residence in the United States; and corporations incorporated in the United States, but not including those entities that are openly acknowledged by a foreign government or governments to be directed and controlled by them (Reference d)

DOCUMENT HISTORY

Date	Approved by	Description
1 March 2021	Paul M. Nakasone, General, U.S. Army; Director, NSA/Chief, CSS	Policy issuance
30 July 2021	Chief, Policy	Administrative update to change Glossary term and correct ATSD(IO) title
8 February 2022	Chief, Policy	Administrative update to change ATSD(IO) title to DoD SIOO