NSA/CSS POLICY 12-1
NSA/CSS CIVIL LIBERTIES AND PRIVACY PROGRAM

DATE:	18 November 2021 (See Document History.)
OFFICE OF PRIMARY INTEREST:	Civil Liberties, Privacy, and Transparency (D5), 969-8225 (secure)
RELEASABILITY:	No section of this document shall be released without approval from the Office of Policy (P12). 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:	18 November 2021

PURPOSE AND SCOPE

1. This document establishes policy, outlines procedures, and assigns roles and responsibilities for the comprehensive administration of the NSA/CSS Civil Liberties and Privacy Program in accordance with 42 United States Code (U.S.C.) 2000ee-1, "Privacy and Civil Liberties Officers" (Reference a), the Privacy Act of 1974 (Reference b), and the directives prescribed in References c–hh. It incorporates and references NSA/CSS processes and procedures that support and protect *civil liberties* and privacy of individuals who may be affected by NSA/CSS activities.

2. This policy applies to all NSA/CSS *affiliates*. Protecting civil liberties and the privacy of *U.S. persons* and others is a responsibility that is shared across all NSA/CSS organizations and by all affiliates.

(U) POLICY

3. NSA/CSS shall protect civil liberties and privacy to the full extent required by law, regulation, and policy and as reflected in NSA/CSS core values: commitment to service, respect for the law, integrity, transparency, respect for people, and accountability. NSA/CSS shall develop and adhere to policies that protect civil liberties and privacy, manage civil liberties and privacy risks at all levels of decision making, and conduct oversight and reporting of civil liberties and privacy aspects of all activities.

4. The Director, NSA/Chief, CSS (DIRNSA/CHCSS) designates the NSA/CSS Director, Civil Liberties, Privacy, and Transparency (CLPT, D5) to serve as both the senior official responsible for the protection of civil liberties and privacy as required by 42 U.S.C. 2000ee-1

(Reference a) and Intelligence Community Directive (ICD) number 107, "Civil Liberties, Privacy, and Transparency" (Reference c), and as the *Senior Component Official for Privacy* as required by Department of Defense Instruction (DoDI) 5400.11, "DoD Privacy and Civil Liberties Programs" (Reference d).

(U) PROCEDURES

5. The NSA/CSS Civil Liberties and Privacy Program addresses all NSA/CSS activities (*mission*, mission support, and administrative). The program covers *personally identifiable information (PII)*, including *U.S. person information (USPI)*, in both *national security systems (NSS)* and non-NSS. PII that is collected, disseminated, processed, and/or stored in computer-based formats, hard copy, or in any other media is included. The program consists of seven main activities per 42 U.S.C. 2000ee-1 (Reference a) and DoDI 5400.11 (Reference d) and is designed to:

a. Advise the NSA/CSS Board of Directors and senior leaders regarding the protection of civil liberties and privacy;

b. Review and assess policy, procedures, technology, and operations and advise on incorporating civil liberties and privacy protections and safeguards in mission, mission-support, and administrative systems;

c. Maintain an effective mechanism for receiving complaints or indications of possible abuses of civil liberties and privacy;

d. Provide training and guidance to NSA/CSS affiliates regarding their responsibilities to identify and protect PII, including USPI, under the Privacy Act of 1974 (Reference b), DoDI 5400.11 (Reference d), Executive Order 12333, "United States Intelligence Activities" (Reference e), DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities" (Reference f), and any other relevant laws, regulations, and policies;

e. Receive and respond to *privacy incidents* involving actual or potential *breaches* of PII in classified and unclassified environments and comply with reporting requirements;

f. Periodically review and investigate NSA/CSS policies, procedures, and operations to determine whether they incorporate the protections and safeguards needed to protect civil liberties and privacy; and

g. Provide appropriate transparency into the civil liberties and privacy protections present in NSA/CSS activities to mission partners; executive, legislative, and judicial branch overseers; and the American public, including reporting independently to DIRNSA/CHCSS and external executive and legislative branch entities regarding the activities of the NSA/CSS CLPT (D5) in accordance with 42 U.S.C. 2000ee-1 (Reference a).

RESPONSIBILITIES

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

6. DIRNSA/CHCSS shall:

a. Appoint a *Civil Liberties and Privacy Officer*, in accordance with 42 U.S.C. 2000ee-1 (Reference a) and ICD 107 (Reference c), who shall report directly to DIRNSA/CHCSS in accordance with 42 U.S.C. 2000ee-1 (Reference a);

b. Appoint a Senior Component Official for Privacy to support the DoD *Senior Agency Official for Privacy (SAOP)* by carrying out the SAOP's duties identified in Office of Management and Budget (OMB) Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act" (Reference g); OMB Circular A-130, "Managing Information as a Strategic Resource" (Reference h); OMB Memorandum M-16-24, "Role and Designation of Senior Agency Officials for Privacy" (Reference i); and DoDI 5400.11 (Reference d);

c. Ensure that all NSA/CSS activities are conducted in a manner that protects civil liberties and privacy in accordance with ICD 107 and DoDI 5400.11 (References c and d);

d. Provide adequate resources to support and maintain an effective civil liberties and privacy program (Reference d) and to ensure that CLPT (D5) has the information, material, and resources needed to fulfill the required functions in accordance with 42 U.S.C. 2000ee-1 (Reference a);

e. Direct that CLPT, the Office of General Counsel (OGC, D2), the Office of the Inspector General (OIG, I), and other offices as appropriate, are given access to information required to protect civil liberties and privacy (Reference c);

f. Provide CLPT with relevant information regarding NSA/CSS missions, plans, programs, policies, tradecraft, operations, and technologies that may have an impact on civil liberties and privacy in support of paragraph 5.f;

g. Prohibit reprisals or the threat of reprisals against individuals who, through established official channels, make complaints or disclose information concerning a possible violation of civil liberties and/or privacy protections or in the administration of programs and operations of NSA/CSS related to efforts to protect the nation from terrorism (References a and d); and

h. Consider specific, limited exceptions to this policy presented by the Director, CLPT.

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

7. The Director, CLPT (D5) shall:

a. Serve as the principal advisor to DIRNSA/CHCSS, Board of Directors members, and other NSA/CSS leaders on policy matters pertaining to civil liberties and privacy, including maintaining an awareness of and engaging with the external civil liberties and privacy communities, both domestic and foreign, and informing NSA/CSS leadership of significant developments or changes in civil liberties and privacy-related policies, public attitudes, best practices, and technologies affecting NSA/CSS and its missions, people, partners, and resources;

b. Assist DIRNSA/CHCSS and others with appropriately incorporating civil liberties and privacy protections when making strategic policy, operational, resource, technology, and *research* decisions by:

1) Developing, issuing, reviewing, interpreting, or contributing to policies, instructions, reports, internal controls, procedures, and guidance to assist NSA/CSS employees and other affiliates with identifying, assessing, and safeguarding PII and/or USPI that may have been intentionally or incidentally collected through authorized NSA/CSS activities;

2) Providing civil liberties and privacy advice and policy guidance, in consultation with OGC (D2) as appropriate, including reviewing requests for new and novel uses of existing authorities and providing guidance related to Attorney General–approved U.S. person privacy procedures and FISA (Foreign Intelligence Surveillance Act) procedures (References a and f);

3) In accordance with 42 U.S.C. 2000ee-1 (Reference a) and DoDI 5400.11 (Reference d), reviewing and advising on legislative proposals intended to retain or enhance NSA/CSS mission authorities before their submission to DoD, the Office of the Director of National Intelligence (ODNI), or Congress;[1]

4) Developing and overseeing the *Civil Liberties and Privacy Assessment (CLPA)* policy and process, including required *privacy impact assessments* (collectively, CLPAs) under the E-Government Act of 2002, that are incorporated into NSA/CSS processes for both NSS and non-NSS systems, programs, activities, and technologies (References d and j);

5) In conjunction with Capabilities (Y), incorporating civil liberties and privacy considerations, protections, and controls into NSS and non-NSS information systems (ISs) using the National Institute of Standards and

[1] These reviews shall consider whether there is a need to protect civil liberties and privacy, whether there is adequate supervision by NSA/CSS to protect civil liberties and privacy when using these authorities, and whether adequate guidelines and oversight exist to properly limit their use.

Technology (NIST) Risk Management Framework (RMF) (Reference k); Committee for National Security Systems Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems Security Overlays," attachment 6, "Privacy Overlay" (Reference l); and the CLPA process;[2]

6) Providing oversight, in consultation with OGC as appropriate, in the implementation of the Privacy Act of 1974 (References b and g) for NSA/CSS, including:

a) Issuing, maintaining, and reviewing *System of Records Notices*;

b) Reviewing current and proposed uses of *Privacy Act Statements*;

c) Reviewing and approving internal and external website policies in accordance with OMB Memoranda M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies" (Reference m); M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications" (Reference n); and M-17-06, "Policies for Federal Agency Public Websites and Digital Services" (Reference o);

d) Serving as the appeals authority for Privacy Act requests (Reference p); and

7) Consulting with the Human Research Protection Program (HRPP)—and referring to the HRPP any NSA/CSS research activities that involve privacy and confidentiality issues whenever these research activities are conducted or supported by NSA/CSS—in accordance with DoDI 3216.02, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Conducted and Supported Research" (Reference q), and NSA/CSS Policy 10-10, "Protecting Human Subjects of Research" (Reference r);

c. Review and advise on the extent and adequacy of civil liberties and privacy training, including training for the protection of PII, including USPI;

d. Periodically investigate and review NSA/CSS policies and activities for civil liberties concerns and privacy protections as appropriate (References a and d);

e. Upon request, provide information to ODNI concerning NSA/CSS activities and requirements related to the protection of civil liberties and privacy;

[2] This RMF guides and informs the categorization of federal information and ISs; the selection, implementation and assessment of privacy controls; the authorization of ISs; and the continuous monitoring of ISs in accordance with the guidance contained in References d, h, i, l, and s–x.)

f. Lead NSA/CSS interactions with the Privacy and Civil Liberties Oversight Board (PCLOB) (Reference a);

g. Represent NSA/CSS on the Intelligence Community's Civil Liberties and Privacy Council (Reference c);

h. Develop and maintain policy and procedures for responding to breaches of PII and process reported or suspected breaches of PII in accordance with applicable laws and policies, including DoDI 5400.11 (Reference d) and NSA/CSS Policy 6-23, "Reporting and Handling of NSA/CSS Information System Security Incidents" (Reference y);

i. Develop, promulgate, and maintain procedures for NSA/CSS to receive, evaluate, respond to, and provide redress for complaints from individuals who allege that NSA/CSS activities have violated their civil liberties or privacy (References a, c, d, and z) by:

1) Ensuring that complaints or indications of possible abuses of civil liberties and/or privacy are documented, reviewed, referred when applicable, assessed, investigated, responded to, resolved as appropriate, and reported in accordance with 42 U.S.C. 2000ee-1 (Reference a);

2) Developing and coordinating timely NSA/CSS responses to ODNI regarding Privacy Shield Agreement requests in accordance with NSA/CSS Policy Memorandum 2017-01, "Review of Allegations of Improper Signals Intelligence Activity under the Privacy Shield Agreement" (Reference z), or successor policy; and

3) Providing whistleblower protections in accordance with 42 U.S.C. 2000ee-1 (Reference a);

j. Develop, promulgate, and maintain procedures to coordinate referrals of civil liberties and privacy complaints to the NSA/CSS Intelligence Oversight Officer (IOO) to the extent they may involve *questionable intelligence activities (QIAs)* and *significant or highly sensitive matters (S/HSMs)* (Reference aa);

k. Develop, promulgate, and maintain procedures to coordinate referrals of civil liberties and privacy complaints to the OIG (I) when criteria established by the OIG have been met, consistent with the OIG's obligation to protect confidentiality under the Inspector General Act (Reference bb) as amended and the integrity of any OIG inquiry or investigation; and

l. Report as required on the activities of the NSA/CSS Civil Liberties and Privacy Program to DIRNSA/CHCSS; the PCLOB; appropriate congressional committees as specified in 42 U.S.C. 2000ee-1 (Reference a); ODNI; and the Defense Privacy, Civil Liberties, and Transparency Division of DoD.

Director, Workforce Support Activities (WSA, A)

8. The Director, WSA (A) shall:

a. Cultivate civil liberties and privacy awareness in the WSA workforce;

b. Consult with CLPT (D5) to develop, maintain, and implement mandatory, role-based civil liberties and privacy training, and advanced training as appropriate, for NSA/CSS employees and affiliates regarding their responsibilities to limit the collection of PII, protect collected PII, protect civil liberties and privacy, and report and respond to incidents involving potential breaches of PII (Reference d);

c. Incorporate civil liberties and privacy protections into the planning, resourcing, and conduct of all mission, mission-support, and administrative activities;

d. Conduct CLPAs in consultation with CLPT and as may be required by law or advisable as a matter of policy;

e. Coordinate with CLPT and Business Management and Acquisition (BM&A, B) to ensure that contractually required CLPAs are conducted and approved before government acceptance and authorization for operational use of contractor-supplied systems or contractor-developed modifications to existing systems of records on individuals required to accomplish an Agency function; and

f. Detail staff on a continuing rotational basis to assist CLPT.

Director, Business Management and Acquisition (BM&A, B)

9. The Director, BM&A (B) shall:

a. Cultivate civil liberties and privacy awareness in the BM&A workforce;

b. Incorporate civil liberties and privacy protections into the planning, resourcing, and conduct of all mission, mission-support, and administrative activities;

c. Conduct CLPAs in consultation with CLPT (D5) and as may be required by law or advisable as a matter of policy;

d. Consult with the Director, CLPT to ensure that the *information technology* (IT) investment budget program submission incorporates guidance from CLPT in accordance with DoDI 5400.11 (Reference d);

e. Include Privacy Act (Reference b) clauses as prescribed in the Federal Acquisition Regulation and DoD Federal Acquisition Regulation Supplement (References a, b, d, g, h, cc, and dd) in Agency contracts that are supporting the design, development, or operation of a Privacy Act system of records and other IT systems as appropriate;

f. In conjunction with CLPT, OGC (D2), and the responsible directorate, ensure that required CLPAs are conducted before government acceptance and approval of operational use of contractor-supplied IT or contractor-developed modifications to existing systems of records on individuals required to accomplish an Agency function;

g. Ensure that NSA/CSS contractor personnel are properly trained and informed of their Privacy Act (Reference b) responsibilities, including their awareness of their individual responsibilities to safeguard PII; and

h. Detail staff on a continuing rotational basis to assist CLPT.

Director, Cybersecurity (C)

10. The Director, Cybersecurity (C) shall:

a. Cultivate civil liberties and privacy awareness in the Cybersecurity workforce;

b. Incorporate civil liberties and privacy protections into the planning, resourcing, and conduct of all mission, mission-support, and administrative activities;

c. Conduct CLPAs in consultation with CLPT (D5) and as may be required by law or advisable as a matter of policy;

d. Represent NSA/CSS on the NIST Information Security and Privacy Advisory Board as required by 15 U.S.C. §278g-4, "Information Security and Advisory Board" (Reference ee); and

e. Detail staff on a continuing rotational basis to assist CLPT.

Director, Engagement and Policy (E&P, P)

11. The Director, E&P (P) shall:

a. Cultivate civil liberties and privacy awareness in the E&P workforce;

b. Incorporate civil liberties and privacy protections into the planning, resourcing, and conduct of all mission, mission-support, and administrative activities;

c. Conduct CLPAs in consultation with CLPT (D5) and as may be required by law or advisable as a matter of policy;

d. Process Privacy Act requests (Reference p);

e. Ensure civil liberties and privacy considerations consistent with this policy are reflected in NSA/CSS policies as needed, in accordance with NSA/CSS Policy 1-1, "NSA/CSS Policy System" (Reference ff);

f. Once authorized for public release, ensure that information concerning and/or implicating civil liberties and privacy is accessible through a range of appropriate communications channels, including those enabled by new technology;

g. Share applicable congressional notifications for determination as to whether a similar notice should be provided to the PCLOB;

h. Coordinate with OGC (D2) to solicit the views of CLPT regarding pending legislative proposals to retain or enhance mission authority of NSA/CSS before submitting them to DoD, ODNI, or Congress;

i. Provide authoritative metrics, assessments, and subject matter expertise as required in support of CLPT external reporting requirements;

j. Inform CLPT of civil liberties and privacy issues resulting from the implementation of the Comprehensive Mission Compliance Program (CMCP) as required in NSA/CSS Policy 12-2 (Reference aa); and

k. Detail staff on continuing rotational basis to assist CLPT.

Director, Research (R)

12. The Director, Research (R) shall:

a. Cultivate civil liberties and privacy awareness in the Research workforce;

b. Maintain situational awareness of external privacy research;

c. Manage the NSA/CSS HRPP in accordance with NSA/CSS Policy 10-10 (Reference r);

d. Execute NSA/CSS research initiatives to explore and develop privacy-enhancing technologies;

e. Incorporate civil liberties and privacy protections into the planning, resourcing, and conduct of all mission, mission-support, and administrative activities;

f. Conduct CLPAs in consultation with CLPT (D5) and as may be required by law or advisable as a matter of policy; and

g. Detail staff on continuing rotational basis to assist CLPT.

Director, Operations (X)

13. The Director, Operations (X) shall:

a. Cultivate civil liberties and privacy awareness in the Operations workforce;

b. Incorporate civil liberties and privacy protections into the planning, resourcing, and conduct of all mission, mission-support, and administrative activities;

c. Conduct CLPAs in consultation with CLPT (D5) and as may be required by law or advisable as a matter of policy;

d. Through the NSA/CSS Senior Operations Data Officer, incorporate civil liberties and privacy considerations, protections, and controls into data management practices in accordance with the directives contained in References d, h, u, and w; and

e. Detail staff on a continuing rotational basis to assist CLPT.

Director, Capabilities (Y)

14. The Director, Capabilities (Y) shall:

a. Cultivate civil liberties and privacy awareness in the Capabilities workforce;

b. Incorporate civil liberties and privacy protections into the planning, resourcing, and conduct of all mission, mission-support and administrative activities;

c. Assist CLPT (D5) with ensuring that civil liberties and privacy considerations are included early in the planning, resourcing, design, and development cycle of existing and new technology programs (Reference d);

d. In conjunction with CLPT, incorporate civil liberties and privacy considerations, protections, and controls into NSS and non-NSS ISs using the NIST RMF (Reference k), Committee for National Security Systems Instruction No. 1253F (Reference l), and CLPA processes in accordance with the guidance contained in References a, d, h, l, t–x and gg;

e. Assist CLPT with designating which privacy controls will be treated as program management, common IS-specific, or hybrid privacy controls in NSA/CSS systems;

f. Coordinate with CLPT to review and approve the IT investment budget request to ensure that privacy requirements, as well as any associated costs, are explicitly identified and included with respect to any IT resource that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII (References d and v);

g. In conjunction with CLPT, identify assessment methodologies and metrics to review results and effectiveness of civil liberties and privacy controls;

h. Develop and maintain an inventory of NSA/CSS ISs, including high-value assets that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII (References d and hh);

i. Coordinate with CLPT on granting authorization to operate decisions for ISs that hold PII, including USPI;

j. Coordinate with CLPT to ensure that the DoD SAOP is aware of ISs and systems of records containing PII that cannot be appropriately protected or secured and that such systems are given a high priority for upgrade, replacement, or retirement in accordance with DoDI 5400.11 (Reference d);

k. Conduct CLPAs in consultation with CLPT and as may be required by law or advisable as a matter of policy;

l. Coordinate with CLPT and BM&A (B) to ensure that contractually required CLPAs are conducted and approved before government acceptance and authorization of operational use of contractor-supplied systems or contractor-developed modifications to existing systems of records on individuals required to accomplish an Agency function; and

m. Detail staff on a continuing rotational basis to assist CLPT.

Deputy Chief, CSS

15. The Deputy Chief, CSS shall:

a. Cultivate civil liberties and privacy awareness in the CSS HQ and workforce;

b. Conduct CLPAs in consultation with CLPT (D5) and as may be required by law or advisable as a matter of policy;

c. Reflect civil liberties and privacy considerations consistent with this policy in organization-specific management directives, guidance, instructions, and working aids as needed; and

d. Designate a point of contact to facilitate engagement with CLPT on civil liberties and privacy issues.

NSA/CSS Chief of Staff (CoS, DC)

16. The NSA/CSS CoS (DC) shall:

a. Cultivate civil liberties and privacy awareness in the directorate (D) and DC workforce;

b. Incorporate civil liberties and privacy protections into the planning, resourcing, and conduct of all mission, mission-support, and administrative activities;

c. Conduct CLPAs in consultation with CLPT (D5) and as may be required by law or advisable as a matter of policy;

d. Secure resources, including personnel, funding, technology, and office space needed to maintain effective civil liberties and privacy programs in accordance with paragraph 6.d. (References a and d); and

e. Provide administrative support and services to CLPT.

Office of General Counsel (OGC, D2)

17. OGC (D2) shall:

a. Provide legal advice, services, and assistance to CLPT (D5) and other Agency officials concerning the Agency's implementation of and adherence to the laws related to the protection of civil liberties and privacy, including the Privacy Act of 1974 (Reference b);

b. Provide legal assessments on all reported or suspected breaches of PII; and

c. Coordinate with CLPT on matters with civil liberties or privacy implications, including special circumstances collection analysis, new or novel uses of authorities, and new legislative proposals.

Director, Diversity, Equality, and Inclusion (DEI, D6)

18. The Director, DEI (D6) shall:

a. Cultivate civil liberties and privacy awareness in Employee Resource Groups and the DEI workforce;

b. Conduct CLPAs in consultation with CLPT (D5) and as may be required by law or advisable as a matter of policy; and

c. Reflect civil liberties and privacy considerations consistent with this policy in organization-specific management directives, guidance, instructions, and working aids as needed.

Chief Risk Officer (D9)

19. The Chief Risk Officer (D9) shall:

a. Incorporate civil liberties and privacy considerations into the NSA/CSS *Enterprise risk framework*; and

b. Engage CLPT (D5) on significant civil liberties and privacy issues arising during the risk assessment and management process in accordance with NSA/CSS Policy 1-71, "Enterprise Risk Management" (Reference gg).

Office of the Inspector General (OIG, I)

20. OIG (I) shall cultivate civil liberties and privacy awareness among the workforce and, acting consistently with the Inspector General Act (Reference bb), shall:

a. Inform CLPT (D5) of matters with civil liberties and privacy implications brought to OIG's attention, consistent with OIG's obligations to protect confidentiality under the Inspector General Act (Reference bb) as amended and the integrity of any OIG inquiry or investigation, and coordinate respective responsibilities;

b. Conduct a periodic review of NSA/CSS privacy programs as part of the OIG annual independent evaluation consistent with the Federal Information Security Modernization Act of 2014 (Reference x); and

c. Maintain a system of records that complies with the Privacy Act of 1974 (Reference b) and notify CLPT of any breaches of PII.

NSA/CSS Intelligence Oversight Officer (IOO)

21. The NSA/CSS IOO shall, in accordance with Policy 12-2, "NSA/CSS Mission Compliance and Intelligence Oversight" (Reference aa), engage CLPT (D5) in the assessment of civil liberty and privacy issues when reviewing and substantiating potential mission compliance incidents, QIAs, and/or S/HSMs, even if the mission activity was deemed to be compliant.

NSA/CSS Cryptologic Center (CC) Commanders/Chiefs and Extended Enterprise Leaders

22. NSA/CSS CC commanders/chiefs and extended Enterprise leaders shall:

a. Cultivate civil liberties and privacy awareness within their respective workforces;

b. Incorporate civil liberties and privacy protections into the planning, resourcing, and conduct of all mission, mission-support, and administrative activities;

c. Conduct CLPAs in consultation with CLPT (D5) and as may be required by law or advisable as a matter of policy;

d. Reflect civil liberties and privacy considerations consistent with this policy in organization-specific management directives, guidance, instructions, and working aids as needed; and

e. Designate a point of contact to facilitate engagement with CLPT on civil liberties and privacy issues.

(U) REFERENCES

a. 42 U.S.C. 2000ee-1, "Privacy and Civil Liberties Officers," as amended 19 January 2018

b. 5 U.S.C. §552a, the Privacy Act of 1974, as amended

c. ICD 107, "Civil Liberties and Privacy," dated 28 February 2018

d.) DoDI 5400.11, "DoD Privacy and Civil Liberties Programs," dated 29 January 2019

e. Executive Order 12333, "United States Intelligence Activities," as amended

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

g. OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," dated 23 December 2016

h. OMB Circular A-130, "Managing Information as a Strategic Resource," dated 28 July 2016

i. OMB Memorandum M-16-24, "Role and Designation of Senior Agency Officials for Privacy" dated 15 September 2016

j. Section 208 of Public Law 107-347, "The E-Government Act of 2002 Privacy Impact Assessments," 44 U.S.C. §§3601-3606

k. National Institute of Standards and Technology, Risk Management Framework, dated April 2018

l. Committee on National Security Systems Instruction 1253F, "Security Categorization and Control Selection for National Security Systems Security Overlays," attachment 6, "Privacy Overlay," dated 23 April 2015

m. OMB Memorandum M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies," dated 25 June 2010

n. OMB Memorandum 10-23, "Guidance for Agency Use of Third-Party Websites and Applications," dated 23 June 2010

o. OMB Memorandum 17-06, "Policies for Federal Agency Public Websites and Digital Services," dated 08 November 2016

p. Those portions of NSA/CSS Policy 1-34, "Implementation of the Privacy Act of 1974," dated 30 October 2020 that address the processing of Privacy Act requests

q. DoDI 3216.02, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Conducted and Supported Research," dated 08 November 2011

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

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

t. DoDI 5400.16, "Privacy Impact Assessment Guidance," dated 12 February 2009

u. NIST SP 800-53, revision 5, "Security and Privacy Controls for Information Systems and Organizations," dated 10 December 2020

v. OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," dated 15 July 2016

w. NSA/CSS Policy 6-3 "Information System Security Authorization Using the Risk Management Framework," dated 30 August 2019

x. Federal Information Security Modernization Act of 2014

y. NSA/CSS Policy 6-23, "Reporting and Handling of NSA/CSS Information System Security Incidents," dated 20 December 2019

z. NSA/CSS Policy Memorandum 2017-01, "Review of Allegations of Improper Signals Intelligence Activity under the Privacy Shield Agreement," dated 29 June 2021

aa. NSA/CSS Policy 12-2, "NSA/CSS Mission Compliance and Intelligence Oversight," dated 30 July 2021

bb. The Inspector General Act of 1978, as amended

cc. Federal Acquisition Regulation part 24.3, "Protection of Privacy and Freedom of Information," dated 10 March 2021

dd. DoD Federal Acquisition Regulation Supplement part 224, "Protection of Privacy and Freedom of Information," dated 20 May 2021

ee. 15 U.S.C. §278g-4, "Information Security and Advisory Board," as amended

ff. NSA/CSS Policy 1-1, "NSA/CSS Policy System," dated 16 April 2021

gg. NSA/CSS Policy 1-71, "Enterprise Risk Management," dated 19 March 2021

hh. OMB Memorandum M-17-09, "Management of Federal High Value Assets," dated 9 December 2016

GLOSSARY

affiliate—An affiliate is a person employed by, detailed to, assigned to, integrated with, or a tenant of a facility within the NSA/CSS Cryptologic Enterprise and granted access to the Enterprise information technology infrastructure for which the Director, NSA/Chief, CSS has operational information system security responsibility. This includes U.S. Government employees, Service cryptologic component personnel, contractors, consultants, and foreign national partners. (Source: NSA/CSS Policy Glossary)

breach—an incident characterized by the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence in which a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose (Source: Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," dated 3 January 2017)

civil liberties—fundamental rights and freedoms protected by the United States Constitution (Reference d)

Civil Liberties and Privacy Assessment (CLPA)—The CLPA is the process and documentation by which NSA/CSS applies civil liberties and privacy considerations to inform NSA/CSS's decision making at the activity and strategic levels. The CLPA:

a. (U) Provides a common lexicon to identify relevant facts about an activity's data, uses of that data, and existing safeguards;

b. (U) Conducts an accurate, consistent, and independent assessment of the impacts on individuals' CLP and recommends additional safeguards as appropriate;

c. (U) Brings together the facts, impacts, and recommendations about high-impact activities to senior management to facilitate an informed decision; and

d. (U) Provides documentation to support increased transparency within NSA/CSS and, as appropriate, to demonstrate good stewardship of its authorities to overseers and the public (Reference d).

Civil Liberties and Privacy Officer—the senior official, designated by the head of each agency, who has agency-wide responsibility for matters involving the protection of civil liberties and privacy as they relate to activities conducted by the agency and for working with Intelligence Community counterparts as a member of the Civil Liberties and Privacy Council (Reference c)

Enterprise risk framework—a set of root-cause and strategic risks that NSA/CSS may encounter when performing a new or ongoing activity (Reference gg)

information technology (IT)—IT includes any services or equipment, or interconnected system(s) or subsystem(s) of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Agency, including computers, ancillary equipment (including imaging peripherals, input, output, and storage devices as needed for security and surveillance), and peripheral equipment designed to be controlled by the central processing unit of a computer; software, firmware, and similar procedures; services (including cloud computing and help-desk services or other professional services that support any point of the life cycle of the equipment or service); and related resources. For purposes of this definition, IT also includes such services or equipment if used by the Agency directly or used by a contractor under a contract with the Agency that requires its use or, to a significant extent, its use in the performance of a service or the furnishing of a product. IT does not include any equipment that is acquired by a contractor incidental to a contract that does not require its use. (Reference h)

mission—Mission includes signals development, collection, processing, analysis, retention, and dissemination of cybersecurity and signals intelligence (SIGINT) products or services in response to customer information needs. Mission also includes any directed or assigned task or function that supports or enables SIGINT or cybersecurity goals/plans. (Source: NSA/CSS Policy Glossary)

national security system (NSS)—An NSS is any information system (IS) (including any telecommunications system) used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, or equipment that is an integral part of a weapon or weapons system. NSS is also any IS that is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, e.g., payroll, finance, logistics, personnel management applications) or one that is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy. (Source: 44 United States Code §3552 (b)(6))

personally identifiable information (PII)—information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual (Reference h)

Privacy Act Statement—governed by the Privacy Act, a statement on a form used to collect information from an individual or a separate form that can be retained by the individual, which specifies the authority (whether granted by statute or by Executive order of the President) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; the principal purpose or purposes for which the information is intended to be used; the routine uses that may be made of the information; and the effects on the individual, if any, of not providing all or any part of the requested information (Reference b)

privacy impact assessment—an analysis of how information is handled to ensure that the handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks (Source: Office of Management and Budget Memorandum M-03-22)

privacy incident—an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system or that constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable-use policies (Reference h)

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 (Source: DoDD 5148.13, dated April 26, 2017)

research—Research is a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research for purposes of this issuance, whether or not they are conducted or supported under a program that is considered research for other purposes. (Sources: Title 32, Code of Federal Regulations, part 219, Protection of Human Subjects," dated 19 January 2018 and Reference q)

Senior Agency Official for Privacy (SAOP)—the senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals (Reference i)

Senior Component Official for Privacy (SCOP)—The SCOP is the senior official appointed by a Department of Defense (DoD) component head to support the DoD Senior Agency Official for Privacy (SAOP) in carrying out the SAOP's duties identified in OMB Memorandum M-16-24, "Role and Designation of Senior Agency Official for Privacy," dated 15 September 2016. Those duties include agency-wide responsibility for privacy, including implementation of privacy protections; compliance with federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals. SAOP duties also include a central role in overseeing, coordinating, and facilitating the agency's privacy compliance efforts. (Reference d)

significant or highly sensitive matter (S/HSM)—A 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; or systemic compromise, loss, or unauthorized disclosure of protected information. (Source: DoDD 5148.13, "Intelligence Oversight," dated 26 April 2017)

System of Records Notice (SORN)—The SORN is a notice published by an agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system. A SORN may be comprised of a single Federal Register notice addressing all of the required elements that describe the current system of records, or it may be comprised of multiple Federal Register notices that together address all of the required elements. (Reference g)

U.S. person—a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments (Reference f)

U.S. person information (USPI)—USPI is information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons. Determining whether information is reasonably likely to identify one or more specific U.S. persons in a particular context may require a case-by-case assessment by a trained intelligence professional. USPI is not limited to any single category of information or technology. Depending on the context, examples of USPI may include names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone number, and internet protocol address information. (Reference f)

DOCUMENT HISTORY

Date	Approved by	Description
18 November 2021	Paul M. Nakasone, General, U.S. Army; Director, NSA/Chief, CSS	Policy issuance; supersedes those parts of NSA/CSS Policy 1-34, "Implementation of the Privacy Act," dated 30 October 2020 that establish policy, responsibilities, and procedures for protecting the privacy of individuals