(U) NSA/CSS POLICY 12-3 ANNEX C

SUPPLEMENTAL PROCEDURES FOR THE COLLECTION, PROCESSING, QUERYING, RETENTION, AND DISSEMINATION OF SIGNALS INTELLIGENCE INFORMATION AND DATA CONTAINING PERSONAL INFORMATION OF NON-UNITED STATES PERSONS

DATE:	(U) 29 June 2023 (See Document History.)
OFFICE OF PRIMARY INTEREST:	(U) Civil Liberties, Privacy, and Transparency (D5), 969-8225 (secure)
RELEASABILITY:	(U) 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:	(U) Paul M. Nakasone, General, U.S. Army; Director, NSA/Chief, CSS
ISSUED:	(U) 29 June 2023

(U) PURPOSE AND SCOPE

1. (U) This policy prescribes binding policy guidance for NSA/CSS personnel and other members of the United States Signals Intelligence (SIGINT) System (USSS) that implements Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities" (Reference a), and National Security Memorandum (NSM)-14, "National Security Memorandum on Partial Revocation of Presidential Policy Directive 28" (Reference b), which revoked Presidential Policy Directive (PPD) 28, "Signals Intelligence Activities" (Reference c), except for sections 3 and 6 of that directive and the Classified Annex to that directive, which remain in effect.

2. (U) The Supplemental Procedures included in this policy address the privacy and civil liberties safeguards required by Executive Order 14086 (Reference a) for U.S. SIGINT activities, including orders of and procedures approved by the Foreign Intelligence Surveillance Court. These Supplemental Procedures must be followed for all SIGINT activities of NSA/CSS or the USSS authorized under Executive Order 12333, "United States Intelligence Activities" (Reference d), the Foreign Intelligence Surveillance Act (Reference e), or other authorities.

3. (U) This policy applies to all NSA/CSS employees and all elements of the USSS and shall be applied consistent with the scope of PPD-28's (Reference c) application to such activities prior to PPD-28's partial revocation by NSM-14 (Reference b).

4. (U) If an NSA/CSS official determines that a departure from these procedures is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, they may approve an emergency departure from these procedures but must notify the Director, NSA/Chief, Central Security Service (DIRNSA/CHCSS), the NSA General Counsel (D2), and the NSA Civil Liberties, Privacy, and Transparency (CLPT, D5) Director as soon thereafter as possible. The NSA General Counsel will provide prompt written notice of any departures stating why advance approval was not possible and describing the actions taken to ensure activities were conducted lawfully to the Office of the Director of National Intelligence (ODNI) General Counsel and the Assistant Attorney General for National Security.

(U) POLICY

5. (U) In recognition that SIGINT activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information as required by Executive Order 14086 (Reference a), the USSS shall:

a. (U) Conduct SIGINT collection activities only following a determination that a specific SIGINT collection activity, based on a reasonable assessment of all relevant factors, is necessary to advance a validated intelligence priority in the National Intelligence Priorities Framework (NIPF) or any successor framework (as determined in accordance with the terms of the National Security Act of 1947, as amended, (Reference f) and other applicable laws and policy direction), although SIGINT does not have to be the sole means available or used for advancing aspects of the validated intelligence priority;

b. (U) Conduct SIGINT activities only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside;

c. (U) Conduct SIGINT collection activities only in pursuit of one or more of the legitimate objectives listed in section 2(b)(i) of Executive Order 14086 (Reference a);

d. (U) Conduct SIGINT collection activities only as validated in accordance with the process identified in section 2(b)(iii) of Executive Order 14086 (Reference a); and

e. (U) Not conduct SIGINT collection activities for the purposes of prohibited objectives listed in section 2 of Executive Order 14086 (Reference a), including for the purposes of:

1) (U) suppressing or burdening criticism or dissent, or the free expression of ideas or political opinions by individuals or the press;

2) (U) suppressing or restricting legitimate privacy interests;

3) (U) suppressing or restricting a right to legal counsel;

4) (U) disadvantaging persons based on their ethnicity, race, color, gender, gender identity, sexual orientation, or religion; or

5) (U) affording a competitive advantage to United States companies or United States business sectors commercially.

6. (U) SIGINT collection activities shall be as tailored as feasible to advance foreign intelligence requirements that have been approved in the manner prescribed by Executive Order 14086 (Reference a), National Security Act of 1947 (Reference f), and other applicable laws and policy direction.

(U) SUPPLEMENTAL PROCEDURES

7. (U) The following safeguards, which apply to the collection, processing and querying, retention, and dissemination of SIGINT by any element of NSA/CSS or the USSS, implement the principles articulated in sections 2(a)(ii) and (iii) of Executive Order 14086 (Reference a).

(U) Collection

8. (U) In determining whether to collect SIGINT, all elements of NSA/CSS and the USSS shall consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources. Such alternatives to SIGINT shall be prioritized.

9. (U) Whenever practicable, SIGINT collection will occur through the use of one or more selection terms in order to focus the collection on specific foreign intelligence targets (e.g., a specific, known international terrorist or terrorist group) or specific foreign intelligence topics (e.g., the proliferation of weapons of mass destruction by a foreign power or its agents).

10. (U) **Application of privacy and civil liberties safeguards to the collection of SIGINT**. Consistent with U.S. SIGINT Directive (USSID) 18, "Protection of Civil Liberties and Privacy of U.S. Person Information When Conducting SIGINT Missions" (Reference g), and section 2 of Department of Defense Manual (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 h), targeted SIGINT collection shall be prioritized over bulk SIGINT collection. For example, NSA/CSS will conduct targeted collection using selection terms whenever practicable. NSA shall only engage in bulk collection upon a determination that it is necessary to engage in bulk collection in order to advance a validated intelligence priority. In addition to confirming advancement of a validated intelligence priority and considering alternatives to SIGINT, when conducting collection or

developing SIGINT collection techniques, NSA/CSS employees and USSS personnel are further required to consider all of the following:

a. (U) Methods to limit the types and aspects of the information collected to those necessary and proportionate to one or more of the legitimate objectives listed in section 2 of Executive Order 14086 (Reference a) (or any authorized updates to the list or new priorities established consistent with the criteria in section 2 of Executive Order 14086 (Reference a));

b. (U) Whether mission requirements can be met by filtering non-pertinent information as soon as practicable after collection; and

c. (U) Whether additional approvals or civil liberties and privacy protections are needed to ensure that collection is conducted consistent with the principles listed in section 2(a), including that it is necessary and proportionate to one or more of the legitimate objectives listed in section 2 of Executive Order 14086 (Reference a) (or any authorized updates to the list or new priorities established consistent with the criteria in section 2 of Executive Order 14086 (Reference a)), and, if so, the USSS entities responsible for implementing those requirements. These requirements apply regardless of whether a specific SIGINT collection activity will be performed through targeted collection or bulk collection.

11. (U) **Bulk collection of SIGINT**. Bulk collection may not be undertaken as part of a SIGINT collection activity authorized pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978 (Reference e). Moreover, when SIGINT collection is necessary to advance a validated intelligence priority, targeted collection shall be prioritized over bulk collection. If a determination is made that NSA/CSS or another element of the USSS must engage in bulk collection in order to advance a validated intelligence priority (e.g., an international terrorist target engages in activities to conceal the target's communications methods so bulk collection is necessary to discover how the target is communicating), the bulk collection shall, nevertheless, be as circumscribed as possible, proportionate to the intelligence objective, and occur only for the minimum period of time the collection element determines is necessary to satisfy the objective. Unless further authorized by the President in light of new national security imperatives, such as new or heightened threats to the national security of the United States, information collected through bulk SIGINT collection may only be used for one or more of the following objectives consistent with section 2(c)(ii)(C) of Executive Order 14086 (Reference a):

a. (U) **Counterterrorism**—protecting against terrorism conducted by or on behalf of a foreign government, foreign organization, or foreign person;

b. (U) **Rescue and recovery of captives**—protecting against the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

c. (U) **Hostile foreign or other intelligence activities**—protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of, a foreign government, foreign organization, or foreign person;

d. (U) **Counterproliferation of weapons of mass destruction**—protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of, a foreign government, foreign organization, or foreign person;

e. (U) **Cybersecurity threats**—protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of a foreign government, foreign organization, or foreign person;

f. (U) **Threats of harm**—protecting against threats to the personnel of the United States or of its allies or partners;

g. (U) **Transnational crime**—protecting against transnational criminal threats, including illicit finance and sanction evasion related to one or more of the objectives listed in section 2 of Executive Order 14086 (Reference a).

12. (U) **Bulk SIGINT Collection Considerations**. Consistent with the SIGINT collection considerations included in section 2 of DoDM S-5240.01-A (Reference h), in any circumstance when application of the above procedures results in a determination that it is necessary for the USSS to engage in bulk collection of SIGINT in order to advance a validated intelligence priority, bulk collection must be limited to circumstances where the NSA Director, or designees, in consultation with the NSA CLPT Director, determines all of the following:

a. (U) the information cannot reasonably be obtained by targeted collection or alternatives to SIGINT;

b. (U) the information is necessary to advance a validated intelligence priority identified in section (c)(ii)(B) of Executive Order 14086 (Reference a) or authorized by the President in light of new national security imperatives, such as new or heightened threats to the national security of the United States as provided for at section 2(c)(ii)(C) in Executive Order 14086 (Reference a); and

c. (U) reasonable methods and technical measures to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information, will be applied.

13. (U) Consistent with the SIGINT collection considerations included in section 2 of DoDM S-5240.01-A (Reference h) and section 2(b)(ii)(D) of Executive Order 14086 (Reference a), the data acquired as part of a targeted SIGINT collection activity that temporarily uses data acquired without the use of discriminants (e.g., without specific identifiers or selection terms) may only be used to support the initial technical phase of the targeted SIGINT collection

activity and retained for the short period of time required to complete this phase and thereafter must be deleted.

(U) Processing and Querying

14. (U) **Data security and access**. Consistent with existing requirements in section 6 of DoDM S-5240.01-A (Reference h) and pursuant to requirements in section 2(c)(iii)(B) of Executive Order 14086 (Reference a), all personal information collected through SIGINT shall:

a. (U) Be processed and stored under conditions that include auditing and internal controls to limit access to authorized personnel who have received appropriate training and have a need to know the information to perform their mission;

b. (U) Be accessed only by individuals who have been approved by supervisory or other appropriate personnel; and

c. (U) When no final retention determination has been made, be accessed only in order to make or support such a determination or to conduct authorized administrative, testing, development, security, or oversight functions, including compliance functions.

15. (U) **Queries of SIGINT collection**. Consistent with the SIGINT processing and query requirements included in section 3 of DoDM S-5240.01-A (Reference h), queries of information acquired through SIGINT may be conducted by the USSS for the legitimate objectives of identifying foreign intelligence, counterintelligence, and support to military operations purposes and for the purpose of protecting the safety or enabling the recovery of a person reasonably believed to be held captive outside the United States. Queries of SIGINT obtained pursuant to authorizations issued under the authority of the Foreign Intelligence Surveillance Act (Reference e) must conform to these procedures and any additional requirements imposed by applicable procedures adopted and approved in the manner prescribed by the Foreign Intelligence Surveillance Act (Reference e), including the documentation of justifications, to the extent reasonable, as provided for by this policy.

a. (U) **Queries using selection terms that identify any person**. Further consistent with existing requirements in section 3 of DoDM S-5240.01-A (Reference h), queries using selection terms that identify any person, regardless of nationality or wherever they might reside, shall be designed to defeat, to the extent practicable under the circumstances, the retrieval of personal information that is not relevant, necessary, nor proportionate to advance a validated intelligence priority listed in section 2(a)(ii) of Executive Order 14086 (Reference a) (or any authorized updates to the list or new priorities established consistent with the criteria in section 2 of Executive Order 14086 (Reference a)).

b. (U) **Queries of bulk SIGINT Collection**. In addition to the above requirements, queries of information acquired through bulk SIGINT collection must be consistent with the permissible uses of SIGINT obtained in bulk as specified in section 2(c)(ii) of Executive Order 14086 (Reference a), including taking into account the impact

on the privacy and civil liberties of all persons, regardless of nationality or where they might reside.

(U) Retention

16. (U) **Application of privacy and civil liberties safeguards to the retention of non-U.S. persons' personal information**. Non-U.S. persons' personal information collected through SIGINT may be retained only if the retention of comparable U.S. person information is permitted under section 4 of DoDM S-5240.01-A (Reference h), including the retention periods applicable to unevaluated SIGINT for which no final retention period has been made. Personal information of non-U.S. persons collected through SIGINT that does not meet these requirements shall be deleted. Personal information of a non-U.S. person retained on the basis that it is foreign intelligence must relate to an authorized intelligence requirement and cannot be retained solely because of the non-U.S. person's foreign status.

(U) Dissemination

17. (U) All SIGINT products and services shall be written so as to focus solely on the provision of foreign intelligence to support national and departmental missions, including support for the conduct of military operations, hostage recovery efforts, or like purposes.

18. (U) The USSS may not disseminate personal information collected through SIGINT solely because of the persons' nationality or country of residence or for the purpose of circumventing Executive Order 14086 (Reference a). Disseminations to U.S. Government personnel must be limited to recipients who are reasonably believed to appropriately protect and have a need to know the information. Disseminations to recipients outside of the U.S. Government shall only occur after NSA/CSS and USSS personnel take due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the potential for harmful impact on the person or persons concerned, before disseminating personal information collected through SIGINT.

19. (U) **Application of privacy and civil liberties safeguards to the dissemination of non-U.S. persons' personal information**. Non-U.S. persons' personal information collected through SIGINT, may only be disseminated in accordance with Executive Order 14086 (Reference a) and consistent with existing requirements in section 5 of DoDM S-5240.01-A (Reference h) and other applicable Intelligence Community (IC) and USSS dissemination standards and directives.

20. (U) **Data quality**. Consistent with existing requirements in DoDM S-5240.01-A (Reference h) and Executive Order 14086 (Reference a), for data quality purposes, the USSS elements that handle personal information collected through SIGINT shall include such personal information in intelligence products only as consistent with applicable IC standards of analytic tradecraft, for accuracy and objectivity, as set forth in relevant directives, including IC Directive 203, "Analytic Standards" (Reference i), with a focus on applying standards relating to the quality and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

(U) Oversight and Training

21. (U) **Documentation**. In order to facilitate the oversight processes included in Executive Order 14086 (Reference a), the USSS shall maintain documentation for each of its SIGINT collection activities to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected. The content of any such documentation may vary based on the circumstances, but shall, to the extent reasonable, provide the factual basis under which the USSS has, based on a reasonable assessment of all relevant factors, assessed that the SIGINT collection activity is necessary to advance a validated intelligence priority. For example, the content of documentation will likely differ depending upon the specific type of SIGINT collection activity, the location at which the activity is conducted, and the element of NSA/CSS or the USSS carrying out the SIGINT collection activity. However, consistent with existing requirements in section 5 of DoDM S-5240.01-A (Reference h), NSA/CSS and USSS personnel will document and annually review the use of selection terms as the basis for collection to ensure compliance with applicable authorities, including Executive Order 14086 (Reference a).

22. (U) **Legal, oversight, cybersecurity, and compliance officials**. NSA has multiple senior-level legal, oversight, cybersecurity, and compliance officials, as further addressed in the responsibilities section of this policy, that meet or exceed all requirements of Executive Order 14086 (Reference a), including ensuring that such officials have access to all information pertinent to carrying out their compliance and oversight responsibilities, that appropriate actions are taken to remediate an incident of non-compliance, and that such officials are free from actions designed to impede or improperly influence their oversight responsibilities.

23. (U) **Noncompliance**. As determined by the NSA Director of Compliance, or designee, after coordination with the NSA CLPT Office (D5) and NSA Office of General Counsel (OGC, D2), when a significant issue of noncompliance arises involving personal information of any person, regardless of nationality, collected as a result of SIGINT activities, the issue shall, in addition to any existing reporting requirements, be reported promptly to DIRNSA or DIRNSA's designee, for follow-on reporting to ODNI, DoD, the Department of Justice, and/or the Foreign Intelligence Surveillance Court in accordance with Executive Order 14086 (Reference a), applicable implementing guidance, and other applicable laws, policies, and procedures.

24. (U) **Training**. Consistent with other existing requirements and section 2(c)(iii)(B)(2) of Executive Order 14086 (Reference a), all NSA/CSS employees and USSS personnel with access to unevaluated SIGINT shall receive training that includes knowing and understanding the requirements of Executive Order 14086 (Reference a)). Such training is a prerequisite to initial and continued access and includes policies and procedures for reporting and remediating incidents of noncompliance. Existing PPD-28 (Reference c) training will be updated, as appropriate, to reflect the issuance of Executive Order 14086 and National Security Memorandum 14 (References a and b), and the Supplemental Procedures included in this policy. NSA will monitor completion of training requirements to ensure compliance with this provision.

25. (U) **Redress**. All USSS elements shall provide the ODNI Civil Liberties and Privacy Office (CLPO) with access to any information necessary to conduct the reviews described in

sections 3(c)(i) and 3(d)(i) of Executive Order 14086 (Reference a) consistent with the protection of intelligence sources and methods, and shall not take any actions designed to impede or improperly influence these reviews. All NSA/CSS and USSS personnel shall comply with any CLPO determination to undertake appropriate remediation, subject to any contrary determination of a panel of the U.S. Data Protection Review Court, and, further, shall comply with any determination by a Data Protection Review Court panel to undertake appropriate remediation.

26. (U) **Auditing and Internal Controls**. Consistent with DoDM S-5240.01-A (Reference h), the USSS will create and maintain sufficient auditing records to verify compliance with this annex, and protect auditing records against unauthorized access, modification, or deletion. The USSS will periodically review the effectiveness of its auditing to ensure the key requirements of Executive Order 14086 (Reference a) remain satisfied.

27. (U) **Privacy and Civil Liberties Oversight Board**. The NSA shall provide the ODNI CLPO and the PCLOB with access to information necessary to conduct the annual review of the redress process described in Executive Order 14086 (Reference a), consistent with the protection of sources and methods.

(U) RESPONSIBILITIES

(U) NSA/CSS Office of the Inspector General (OIG, I)

28. (U) The NSA/CSS OIG (I) shall perform the appropriate oversight of NSA/CSS activities to prevent or detect violations of these Supplemental Procedures consistent with the Inspector General Act of 1978, as amended (Reference j).

(U) NSA Office of General Counsel (OGC, D2)

29. (U) The NSA OGC (D2) shall provide legal advice and assistance, as appropriate, regarding the requirements of Executive Order 14086 (Reference a) and the implementation guidance contained in these Supplemental Procedures, including the development of appropriate documentation standards in order to facilitate the oversight processes specified by Executive Order 14086 (Reference a). The OGC, as appropriate, will coordinate closely with the NSA CLPT (D5) to ensure alignment and coordination for the Agency's implementation of the privacy and civil liberties safeguards required by Executive Order 14086 (Reference a).

(U) NSA/CSS Civil Liberties, Privacy, and Transparency (CLPT, D5)

30. (U) NSA/CSS CLPT (D5) shall:

a. (U) Provide civil liberties and privacy advice and assistance regarding the requirements of Executive Order 14086 (Reference a) and the implementation guidance contained in these Supplemental Procedures, including developing appropriate documentation standards in order to facilitate the oversight process specified in Executive Order 14086 (Reference a);

b. (U) Implement the guidance issued by ODNI CLPO for conducting SIGINT reviews and assessments from a civil liberties and privacy perspective under IC Directive 126, "Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086" (Reference k), including assessments of the adequacy of safeguards to protect personal information that are either proposed or in place for new or unique SIGINT collection programs; and

c. (U) Receive, review, and respond to redress requests from ODNI CLPO, including providing ODNI CLPO with access to information necessary to conduct the reviews described in either section 3(c)(i) or section 3(d)(i) of Executive Order 14086 (Reference a) consistent with the protection of intelligence sources and methods.

(U) Risk Management Office (RMO, D9)

31. (U) The RMO (D9) shall provide risk management advice and assistance regarding the requirements of Executive Order 14086 (Reference a) and the implementation guidance contained in these procedures consistent with the implementation of risk management efforts across NSA/CSS.

(U) Director, Operations (X) and Director, Cybersecurity (C)

32. (U) The Director, Operations (X), and, as applicable and relevant, the Director, Cybersecurity (C) shall:

a. (U) Inform and ensure all personnel conducting SIGINT activities under DIRNSA's authorities understand their responsibilities and maintain a high degree of awareness and sensitivity to the requirements of these Supplemental Procedures;

b. (U) Apply the provisions of these Supplemental Procedures to all SIGINT activities governed by Executive Order 14086 (Reference a) that are conducted under DIRNSA's authorities;

c. (U) Conduct necessary reviews of SIGINT production activities and practices, including development of required assessments, governed by Executive Order 14086 (Reference a) to ensure consistency with these Supplemental Procedures. These reviews will include periodic auditing against the standards required by these Supplemental Procedures;

d. Participate in the development of appropriate documentation standards in order to facilitate the oversight processes specified by Executive Order 14086 (Reference a); and

e. (U) Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the OGC (D2). All activities that raise questions of law or the proper interpretation of these Supplemental Procedures must be reviewed by the OGC prior to acceptance or execution.

(U) Chief, Compliance (P7)

33. (U) The Chief, Compliance (P7), shall provide compliance advice, formal and updated training, and assistance regarding the requirements of Executive Order 14086 (Reference a) and the implementation guidance contained in these procedures, including developing appropriate documentation standards in order to facilitate the compliance and oversight process specified in Executive Order 14086 (Reference a).

(U) Chief Information Officer (CIO, Y)

34. (U) The CIO (Y) shall ensure that proper data security, access, and quality is maintained within all capabilities operated by NSA/CSS.

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

35. (U) Directors, the NSA/CSS Chief of Staff, and extended Enterprise commanders/chiefs shall:

a. (U) Recognize, understand, and execute NSA/CSS authorities in a compliant manner;

b. (U) 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 in accordance with NSA/CSS Policy 12-2, "NSA/CSS Mission Compliance and Intelligence Oversight" (Reference l);

c. (U) Enable training for NSA/CSS employees and USSS personnel who have access to operations information regarding DoD Directive (DoDD) 5148.13, "Intelligence Oversight" (Reference m), DoDM 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities" (Reference n), DoDM S-5240.01-A (Reference h), and this policy on the requirements for collecting, processing, querying, retaining, and disseminating SIGINT information;

d. (U) Apply the provisions of this policy to all SIGINT mission activities under their cognizance and ensure that all publications, directives, and instructions for which they are responsible are in compliance with this policy;

e. (U) Conduct a periodic review of the SIGINT 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. (U) Ensure that all new 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 NSA/CSS CLPT (D5) as required and comport with Compliance (P7) requirements and controls;

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

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

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

(U) NSA/CSS Employees and United States Signals Intelligence System (USSS) Personnel:

36. (U) NSA/CSS employees and USSS personnel shall:

a. (U) Implement these Supplemental Procedures upon publication;

b. (U) Immediately inform the Director, Operations (X) staff of any tasking or instructions that appear to require actions at variance with these Supplemental Procedures;

c. (U) In accordance with existing procedures, report to the OIG (I) and consult with the OGC on all activities that may raise a question of compliance with these Supplemental Procedures;

d. (U) If a non-U.S. person's personal information is improperly stored, accessed, collected, analyzed, queried, retained or disseminated, then the incident must be reported to the NSA/CSS Office of Compliance for Cybersecurity and Operations (P75) via NSA's Incident Reporting Tool (go IRT) (or any successor tool) within 24 hours upon recognition;

e. (U) Comply with the procedures outlined in DoDM 5240.01 (Reference n) and DoDM S-5240.01-A (Reference h);

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

g. (U) Conduct mission activities lawfully and in a manner that protects privacy and civil liberties in accordance with this policy and USSID 18 (Reference g), including the compliance and oversight requirements in NSA/CSS Policy 12-2 (Reference l); and

h. (U) Report potential SIGINT mission compliance incidents, Questionable Intelligence Activities (QIAs), and/or Significant or Highly Sensitive Matters (S/HSMs) as defined in DoDD 5148.13 (Reference m) immediately upon recognition in NSA's IRT (or any successor tool). Any potential S/HSM that is not mission-related must be reported to the NSA Intelligence Oversight Officer (NSA IOO) via the alias DL NSA_IOO.

(U) REFERENCES

a. (U) Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities," dated 7 October 2022

b. (U) NSM-14, "Partial Revocation of Presidential Policy Directive 28," dated 7 October 2022

c. (U) PPD-28, "Signals Intelligence Activities," with Annex: "Policy Review of Sensitive Signals Intelligence Collection Activities," dated 17 January 2014

d. (U) Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981, and as amended

e. (U) Foreign Intelligence Surveillance Act of 1978, 50 U.S. Code (U.S.C.) §§1801 et seq., as amended

f. (U) National Security Act of 1947, 50 U.S.C. §§3001 et seq., as amended

g. (U) USSID 18, "Protection of Civil Liberties and Privacy of U.S. Person Information When Conducting SIGINT Missions," issued 10 January 2022

h. (U) 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 Executive Order 12333," dated 7 January 2021

i. (U) Intelligence Community Directive 203, "Analytic Standards", dated 2 January 2015

j. (U) United States Code, Title 5, Section 401-424, "Inspector General Act of 1978", as amended, dated 12 October 1978

k. (U) Intelligence Community Directive 126, "Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086," 6 December 2022

l. (U) NSA/CSS Policy 12-2, "NSA/CSS Mission Compliance and Intelligence Oversight," dated 16 May 2022

m. (U) DoDD 5148.13, "Intelligence Oversight," dated 26 April 2017

n. (U) DoDM 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," dated 8 August 2016

o. (U) 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," dated 10 January 2022

(U) GLOSSARY

(U) This annex carries forward the same definitions provided in 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" (Reference o). Any terms not otherwise defined in DoDD 5148.13 (Reference m) that are included in these Supplemental Procedures shall have the same definitions contained in Executive Order 14086 (Reference a), Executive Order 12333 (Reference d), DoDM 5240.01 (Reference n), and DoDM S-5240.01-A (Reference h).

(U) DOCUMENT HISTORY

(U//FOUO)

Date	Approved by	Description
29 June 2023	Paul M. Nakasone, General, U.S. Army; Director, NSA/Chief, CSS	Policy 12-3 Annex C issuance

(U//FOUO)