BY THE ORDER OF THE COMMANDER NORTH AMERICAN AEROSPACE DEFENSE COMMAND (NORAD) AND UNITED STATES NORTHERN COMMAND (USNORTHCOM)

NORAD AND USNORTHCOM HEADQUARTERS OPERATING INSTRUCTION 31-184

9 MARCH 2012

Security

NORAD AND USNORTHCOM SPECIAL ACCESS PROGRAM CONTROL OFFICE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: NORAD and USNORTHCOM publications and forms are available on the Headquarters NORAD and USNORTHCOM portal page for downloading at https://operations.noradnorthcom.mil/C1/Library/Web%20Part%20Pages%20%20Functional%20Topics/Command%20Publications%20and%20Forms.aspx All other publications and forms are available at the organizations website.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: N-NC/J39 Certified by: N-NC/CS (Maj Gen Howard N. Thompson)

Pages: 11

This Headquarters Operating Instruction implements Chairman Joint Chiefs of Staff (CJCS) Instruction 5250.01, ***Special Access Program (SAP) Policy***. This Instruction implements policy, assigns responsibilities and authorities for the management, administration and oversight of all SAPs at NORAD and USNORTHCOM. This instruction applies to all military, civilian and contractors assigned to HQ NORAD and USNORTHCOM. It does not apply to National Guard and Reserve units. Send recommendations to change, add, or delete information in this instruction to the Office of Primary Responsibility (OPR) using the AF Form 847, ***Recommendation for Change of Publication;*** route AF Form 847 from the field through the appropriate functional's chain of command. This publication may not be supplemented. Maintain and dispose of records created as a result of prescribed processes in accordance with the Chairman Joint Chiefs of Staff Manual (CJCSM) 5760.01A, ***Joint Staff and Combatant Command Records Management Manual: Volume I (Procedures)*** and CJCSM 5760.01, ***Joint Staff and Combatant Command Records Management Manual: Volume II (Disposition Schedule).*** The glossary of references and supporting information are located within **Attachment 1.**

1. **Purpose.** The CDR NORAD and USNORTHCOM has directed that the N-NC/J39/Special Access Program Control Office (SAPCO) be the Commands' centralized office responsible for the management, administration, oversight and security of all SAPs. This will eliminate confusion, duplication of duties and responsibilities and streamline access for NORAD and USNORTHCOM personnel to the SAPs necessary for the performance of essential duties and missions assigned to the Commands.

2. Policy.

2.1. NORAD and USNORTHCOM has designated the SAPCO to serve as the single entry point for SAPs into the Command. The SAPCO represents the Commander and is responsible for coordinating and overseeing SAP activity within the Commands. Any agency, component, organization, or program desiring to access command personnel to a SAP, must contact the SAPCO before taking any action to introduce their program into the Commands.

2.2. SAP information and material must be protected at all times in a manner commensurate with its classification, sensitivity and in accordance with appropriate security directives. This HOI prescribes requirements, restrictions and other enhanced procedures and safeguards that are necessary to prevent unauthorized disclosure of classified SAP information and to control distribution of SAP classified information to only those authorized to receive such information.

3. Responsibilities.

3.1. NORAD and USNORTHCOM Chief of Staff. Responsible for ensuring implementation of SAP policies and procedures as outlined in this HOI and cited references. Designate in writing a NORAD and USNORTHCOM Special Access Program Control Officer (SAPCON) and Special Access Program Security Manager (SAPSM). Appoint Investigating Officials for SAP Security Investigations.

3.2. Executive and Support Staff. Notify the SAPCO of all SAP-related meetings, briefings (including contractors), staff packages and other activities that support the Commander, Deputy Commanders and Chief of Staff.

3.3. NORAD and USNORTHCOM Directorates. Directors will:

3.3.1. Ensure all personnel nominated for access to SAP material have a legitimate need-to-know (NTK) and the ability to materially contribute to the program requested. Ensure the number of personnel nominated for access to SAPs is the minimum number required to complete their duties and responsibilities without a gap in coverage in their subject matter areas.

3.3.2. Ensure that all security incidents involving SAP information/material are reported to the SAPSM within 24 hours of its occurrence.

3.3.3. Coordinate all SAP actions through the SAPCO.

3.4. NORAD and USNORTHCOM J39. Ensure adequate manning with competent security personnel to implement the enhanced security measures required for SAPs in accordance with the appropriate policies and directives. Provide a SAP Facility (SAPF) for the SAPCO separate from other SAPFs.

3.5. NORAD and USNORTHCOM SAP Control Office (SAPCO).

3.5.1. Serves as the Commands' single point of entry for all SAPs.

3.5.2. Serves as the designated proponent for developing and implementing policies and procedures for NORAD and USNORTHCOM related to security, execution, management and administration of SAPs.

3.5.3. Ensures the management of SAPs is in accordance with DOD Instruction O-5205.11 and DOD Overprint to NISPOMSUP and the Standard Operating Procedures (SOP).

3.5.4. Provides security guidance and support to NORAD and USNORTHCOM components executing SAPs. This support includes SAP access eligibility determination for personnel, preparing and processing program access requests and facilitating Automated Information Systems (AIS) and facility accreditation.

3.6. NORAD and USNORTHCOM SAP Control Officer (SAPCON). The SAPCON is appointed in writing, by the Chief of Staff and ensures NORAD and USNORTHCOM compliance with CJCSI 5250.01 and other SAP Policy and directives. The mission of the SAPCON is to seek and provide access to, and ensure security compliance for, SAPs for the Commander and his staff. The SAPCON ensures oversight, management and coordination of all SAP activities across NORAD and USNORTHCOM functional and mission areas. The SAPCON will:

3.6.1. Advise and support the Commander, Deputy Commander, Chief of Staff and Directors for SAP content and security matters. The SAPCON will have sufficient authority to speak on behalf of the Commands regarding SAP matters and to coordinate SAP actions as tasked by the Commander. Provide oversight and ensure unity of effort for SAPs across all mission areas identified by the Unified Command Plan (UCP) mission tasking and in keeping with the Commander's guidance and priorities.

3.6.2. Maintain access to all SAPs on behalf of the Commander and serve as the NORAD and USNORTHCOM primary technical advisor for SAPs. Search out the various SAP activities and capabilities that can either directly or indirectly support NORAD and USNORTHCOM missions to determine relevance to the Commands' requirements and UCP responsibilities. Coordinate with all applicable SAP providers to gain insight into these programs and coordinate/facilitate access for NORAD and USNORTHCOM leadership and action officers as required.

3.6.3. Act as NORAD and USNORTHCOM SAP Executive Committee (EXCOM) secretariat and utilize the SAP EXCOM and other elements of the staff to accomplish required SAP tasking and activities. During operations and exercises, coordinate SAP activities in support of the NORAD and USNORTHCOM Campaign Plans and Commander's objectives. Coordinate military utility assessments (MUAs) of mission-related SAPs and develop the NORAD and USNORTHCOM Annual SAP Report.

3.6.4. Standardize, manage and coordinate all SAP activities within both Commands and coordinate with other Combatant Commands, the Services, the Joint Staff, the Offices of the Secretary of Defense (OSD) and other Agencies and Organizations, as required. For those interagency activities that have SAP counterparts, the SAPCON will coordinate command staffing activities, as well as accesses and security oversight. Use accredited facilities, containers, and AIS for discussion, storage, transfer and protection of SAP information and relies on the SAPSM as primary technical advisor for SAP security matters.

3.6.5. Ensure appropriate NORAD and USNORTHCOM personnel gain access to and knowledge of current and emerging SAP information related to the Commands' UCP assigned missions. The SAPCON will have access to and ensure currency of national access databases and security information to ensure NORAD and USNORTHCOM personnel can conduct assigned SAP-related duties.

3.7. NORAD and USNORTHCOM SAP Security Manager (SAPSM). The SAPSM is appointed, in writing, by the Chief of Staff. The SAPSM is directed by and ensures NORAD and USNORTHCOM compliance with CJCSI 5250.01 and other SAP Policy and directives to ensure

all necessary security safeguards of NORAD and USNORTHCOM SAP personnel, facilities, materials, information and information systems. The SAPSM will be trained in personnel, physical and information security for SAPs. The SAPSM will:

3.7.1. Be appointed as the sole NORAD and USNORTHCOM SAP Facility Accreditor, ensuring that all command facilities that store, handle, process and/or discuss SAP information are conducted within an accredited SAP Facility (SAPF) and that construction standards of all SAPFs are maintained. Ensure that all NORAD and USNORTHCOM SAPFs are inspected IAW appropriate directives.

3.7.2. Serve as the NORAD and USNORTHCOM Designated Approving Authority (DAA) for SAP Protection Level (PL) 1 and 2 AISs. Ensure that all SAP AISs that operate within NORAD and USNORTHCOM facilities are accredited by the SAPSM or appropriate accrediting authority.

3.7.3. Ensure mandated initial and annual Tier Reviews and refresher training for all NORAD and USNORTHCOM and component SAP accessed personnel is conducted.

3.7.4. Validate Program Access Requests (PARs) and submit through the JS SAPCO.

3.7.5. Ensure all personnel access briefs/debriefs/status for SAPs are entered in the Defense Common Access Database System (DCADS) to facilitate access verification.

3.7.6. Coordinate the introduction of any new SAP activity into NORAD and USNORTHCOM with the Joint Staff SAPCO.

3.7.7. Report all security incidents involving SAP material within 24 hours to the Joint Staff SAPCO or the appropriate control office. Investigate and report the results of security incidents and violations IAW the provisions of this instruction and applicable references.

3.7.8. Ensure that all SAPFs operating within NORAD and USNORTHCOM establish a document control program and comply with all program security requirements. Ensure that inventories are conducted and submitted to appropriate authorities.

3.7.9. Perform Annual Security Compliance Inspections and/or periodic assistance visits of all NORAD and USNORTHCOM SAPFs to ensure compliance with appropriate directives. Submit a formal report to the inspected organization as well as the program office and monitor corrective actions as necessary.

3.7.10. Develop and maintain SAP security Standard Operating Procedures (SOP) and emergency procedures for all NORAD and USNORTHCOM SAPFs.

3.7.11. Conduct SAP indoctrinations and briefings.

3.7.12. Oversee all NORAD and USNORTHCOM Government SAP Security Officers (GSSO) and ensure all security documentation is current and maintained IAW the provisions of this instruction and applicable references.

3.7.13. Advise and provide guidance on classification and marking of SAP material.

3.7.14. Ensure that all storage, handling and/or discussion of SAP information and/or material is conducted in a NORAD and USNORTHCOM accredited SAPF or SAP Temporary Secure Working Area (TSWA), as appropriate.

3.7.15. Ensure that all Automated Information System (AIS) used for the processing or communication of SAP information are accredited by the appropriate SAP Cognizant

Authority, located in an accredited SAPF and a copy of the Authority To Operate (ATO) is documented in the NORAD and USNORTHCOM SAPCON Information System Security Plan (ISSP). Conduct and/or review the certification and accreditation testing and ensure all software, hardware and firmware changes are implemented based on applicable guidance.

3.8. Government SAP Security Officer (GSSO). The SAPSM will appoint in writing at least one GSSO for each of the Commands' SAPFs. These personnel will be responsible to the SAPSM for the daily management of all SAP security at their respective SAPF. The GSSO will:

3.8.1. Possess access to all SAPs assigned to the facility(s) for which they are responsible.

3.8.2. Provide security administration and management for their SAPF.

3.8.3. Ensure personnel nominated for access to a SAP meet the prerequisite personnel clearance and/or investigative requirements specified.

3.8.4. Ensure strict adherence to the provisions of this instruction and other applicable security regulations and guidance.

3.8.5. Establish and oversee a classified material control program for each SAP.

3.8.6. Conduct an annual inventory of accountable classified material.

3.8.7. Monitor reproduction and/or duplication and destruction of SAP information.

3.8.8. Ensure adherence to special communications capabilities within the SAPF.

3.9. NORAD and USNORTHCOM Special Technical Operations (STO) Chief.

3.9.1. Responsible for administration of operations and security within NORAD and USNORTHCOM STO Facilities.

3.10. NORAD and USNORTHCOM SAP Program Managers (PM). Due to the level of effort to support testing and evaluation, planning, operations and intelligence missions certain SAPs require that a Command lead be designated to oversee and manage Command equities in the SAP. These Command PMs will coordinate directly with the Service or Agency SAP owner, however, they will work all SAP administrative and security functions through the Command SAPCO in accordance with this HOI. The SAP PMs will:

3.10.1. Act as the Commands' lead and subject matter expert (SME) for the SAP(s) for which they are responsible. Attend SAP Program Management Reviews (PMR) and other meetings and conferences, as required. Provide SAP indoctrination briefings and de-briefings for Command personnel.

3.10.2. Manage the billet structure for their SAP(s). Nominate Command personnel for access to the SAP(s) based on material contribution and NTK. Ensure the number of personnel nominated for access is the minimum number required to complete their duties and responsibilities. Annually, at a minimum, perform a billet scrub to ensure that personnel briefed to the SAP(s) still require access.

3.11. NORAD and USNORTHCOM SAP-Briefed Personnel.

3.11.1. General.

3.11.1.1. Notify SAPCO immediately of any attempts by outside agencies, organizations, etc., to introduce SAP material to Command personnel.

3.11.1.2. Only conduct SAP discussions in designated SAPFs or SAP TSWAs.

3.11.1.3. Notify SAPSM when planning to visit other organizations/contractors with the intent to discuss SAP information. SAPSM will forward a Visit Certification.

3.11.1.4. Ensure that all security incidents involving SAP information/material are reported to the SAPSM within 24 hours of its occurrence.

3.11.2. Program Access. Access to SAPs is a privilege reserved for those personnel whose personal and professional history indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion and sound judgment. Tier Reviews are conducted during the initial and annual SAP access eligibility determination process and to address substantial issues identified that may impact an individual's ability to protect SAP information.

3.11.2.1. Initial Tier Review. Candidates for initial SAP access must submit a copy of their most recent Standard Form (SF)-86, ***Questionnaire for National Security Positions***, to the SAPSM. The SF-86 must be updated to current in one of two ways:

3.11.2.1.1. Ink updates on the original SF-86 with new signatures/dates where indicated, or

3.11.2.1.2. Submit a signed SF-86C, ***Standard Form 86 Certification***.

3.11.2.2. Annual Tier Review. SAP-briefed personnel must annually submit an SF-86C to the SAPSM. This recertification will be accomplished in conjunction with annual SAP security training.

3.11.3. SAP Security Training**.** Security education and training is critical to ensuring SAPs are maintained and protected. All SAP-briefed personnel will accomplish initial SAP Security Training when first accessed to SAP material and annually thereafter. This training will be documented on a SAP Form 17, ***Record of Annual Training***, or its equivalent. All NORAD and USNORTHCOM SAP-briefed personnel will accomplish the following annual security training measures:

3.11.3.1. Review the SAP Annual Refresher Training Security Briefing.

3.11.3.2. Review Critical Protected Information (CPI) and reaffirm NTK/material contribution for the SAPs to which they are briefed.

3.11.4. NORAD and USNORTHCOM SAP-briefed personnel who fail to accomplish Annual SAP Security Training and SF-86 recertification within 30 days of notification will be subject to suspension of SAP access and after 60 days from initial notification will be debriefed from all SAPs.

3.11.5. Random Counter Intelligence (CI) Polygraph (Poly) Screening. All NORAD and USNORTHCOM SAP-briefed personnel are subject to random CI Poly. Failure to submit to a CI-Poly will result in debrief from all SAPs.

3.11.6. Random Inspection of Personal Items. All personnel are subject to random inspections of personal items as they enter and/or exit SAPFs/TSWAs.

3.11.7. Reporting Requirements. The SAPSM must be made aware of any reports which affect the baseline clearance or any change of a personnel security clearance nature involving SAP-briefed personnel. It is the responsibility of each SAP-accessed member to notify the SAPSM of adverse actions that might affect Special Program eligibility and change in duties or duty

title (including, but not limited to PCS, new duty/role, or retirement/separation, financial, criminal activity, etc.).

3.11.7.1. Foreign Contacts. Report close and continuing contact with foreign citizens to the SAPSM. Routine contact with Canadian Forces personnel assigned to NORAD and USNORTHCOM need not be reported so long as that contact is consistent with normal duties and work related functions and does not involve unsolicited queries about SAP material.

3.11.7.2. Foreign Travel. Report all foreign travel (personal and official) to the SAPSM. Personnel conducting foreign travel must complete the ***SAP Form 6, Notification of Foreign Travel*** and submit the completed form prior to departure. Upon return the travelling member will complete and submit the return from travel portion of the Notification of Foreign Travel form. If incidents that require reporting occurred during travel, ensure the SAPSM is notified so that a more in-depth debriefing can be accomplished. The SAPSM will ensure that personnel are given a foreign travel briefing, including general and country specific information and threat advisories, when appropriate, review the proposed itinerary, follow-up on security-related issues and update personnel databases with the foreign travel.

4. General Provisions and Requirements.

4.1. General: NORAD and USNORTHCOM provide operational guidance, planning requirements and advocacy for SAPs that fall within their assigned UCP missions. NORAD and USNORTHCOM also coordinate with, support and are supported by their components in the planning and execution of SAPs, using Integrated Joint Special Technical Operations (IJSTO) as well as processes outlined in this instruction. IJSTO processes are managed by the NORAD and USNORTHCOM STO Chief. The SAPCO manages all SAP activities and maintains coordination authority and overall SAP awareness for the Commands. NORAD and USNORTHCOM component sites each have IJSTO and SAP managers and security officers that coordinate with NORAD and USNORTHCOM SAPCO and STO Chief for their respective organizations.

4.2. SAP Governance. The Special Programs governance structure at NORAD and USNORTHCOM is comprised of the SAP EXCOM and the STO Working Group (STOWG).

4.3. SAPFs. Only facilities that have been accredited as SAPFs are authorized to store, discuss, handle or process SAP material. Only the SAPSM has been delegated to accredit and inspect NORAD and USNORTHCOM facilities at a SAPF or a SAP TSWA level. Accreditation of additional SAPFs or TSWAs will be coordinated with the SAPSM who will work with the Joint Staff SAPCO for approval.

4.3.1. *A SAPF can be located in a Sensitive Compartmented Information Facility (SCIF), but a SCIF is not a SAPF*. NORAD and USNORTHCOM personnel accessed to SAP information will use only approved and accredited SAPFs or TSWAs for SAP discussions. For a current list of SAPFs and SAP TSWAs, contact the SAPSM.

4.4. SAP AIS. Only SAP accredited Information Systems can be used for passing SAP information including SAP Video Teleconferences (VTC). All SAP AIS must reside in a SAPF. *Joint Worldwide Intelligence Communication System (JWICS), SIPR-Net, NIPR-Net and NEN are not authorized for discussion or transmission of SAP material.* Telephonic SAP communications can be conducted on Secure Terminal Equipment (STE) phones at the appropriate classification level, but *only in a SAPF point-to-point with another SAPF*.

4.5. Standard Operating Procedures (SOP). The SAPCO maintains a common SOP for all NORAD and USNORTHCOM SAPFs. Individual SAPF GSSOs are responsible for ensuring compliance with the common SOP in their SAPF. Additionally, they are responsible for ensuring requirements that are unique to their SAPFs are either incorporated in the common SOP or in a supplement. SAPF GSSOs will forward proposed changes to the SOPs and/or supplements to the SAPSM for approval.

4.6. SAP Security Compliance Inspections. All NORAD and USNORTHCOM SAPFs shall be subject to the security compliance inspection process. The SAPSM will conduct annual security inspections. However, if security risks and/or previous inspections warrant additional security oversight, the SAPSM may determine the need to conduct inspections more frequently.

4.7. SAP Security Violations and Infractions. Due to the increased security requirements and limited access for SAPs, all security violations and infractions involving SAP material with be managed by the SAPCO. The SAPCO will coordinate with Command Security to ensure compliance with established processes.

4.7.1. All security incidents involving SAP material must be reported to the SAPCO within 24 hours of its occurrence.

4.7.2. The SAPCON will appoint a Preliminary Inquiry Official who will conduct a preliminary inquiry on all security violations or infractions. This individual will be briefed to the SAP(s) involved. The purpose of a preliminary inquiry is to determine the cause of the violation/infraction, take appropriate action to prevent a recurrence and determine if a formal investigation is required.

4.7.3. If the results of the Preliminary Inquiry indicate that a Security Investigation is required, the Chief of Staff will appoint the Investigation Official. Again this individual will be briefed to the SAP(s) involved.

4.7.4. The SAPCON or SAPSM will provide initial notification of the incident to the owning SAP Program Manager (PM) and/or Program Security Manger (PSM) and provide the results at the conclusion of the inquiry/investigation. If a compromise is found to have occurred, the owning SAP PM and/or PSM will help determine the seriousness of damage to U.S. interests and the appropriate measures to be taken to negate or mitigate the adverse effect of such compromise. When possible, action will be taken to regain custody of documents or material that was compromised. In all cases, appropriate action must be taken to identify the source and reason for the actual or potential compromise and remedial action taken to prevent recurrence.

4.7.5. Reports of security infractions/violations will be filed within the individual's personnel security files maintained by the SAPSM.

4.8. Visit Certification Procedures. SAP visit certifications will be handled exclusively by the SAPCO. *All SAP accessed personnel must make every effort to provide ample advance notification to the SAPSM when visiting other organizations/contractors with the intent to discuss SAP information.* A SAP visit certification request will be made through the SAPSM to the facility to be visited prior to any SAP related visit.

4.9. Couriering SAP Information. The practice of couriering SAP information will only be used as a last resort. If the need arises to courier SAP information, contact the SAPSM to obtain approval and assistance.

4.10. Executive Officers. While it is often standard practice for executive officers to understand many of the issues of their principals, it is not standard practice to access them to SAP material, unless they have a legitimate need-to-know and will make a continuing material contribution to the efforts of their principals.

4.11. Transfer-in-Status (TIS). TIS of SAP accesses are not permitted (for instance for permanent changes of station from or to other duty assignments).

4.12. Double Billeting. Personnel will not be double-billeted except in those circumstances where there is a change of personnel and both individuals need to be briefed in order to transition duties and enable an orderly turnover of responsibility. Double billeting is limited to a specific period of time depending on the type of special program. Double-billeting for the purpose of obtaining additional accesses or "leaping" personnel from billet to billet to avoid the normal process is not authorized.

ANDRÉ VIENS, Major General, RCAF
Director of Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 12968, ***Access to Classified Information,*** 4 Aug 1995

DoD Directive 5205.07, ***Special Access Program (SAP) Policy,*** July 1, 2010

DoD Instruction O-5205.11, ***Management, Administration and Oversight of DoD Special Access Programs (SAPs),*** July 1, 1997

DoD 5220.22-M-Sup 1, ***National Industrial Security Program Operating Manual Supplement,*** 1 February 1995, with Overprint, 1 April 2004

CJCSI 3120.08C, ***Integrated Joint Special Technical Operations (IJSTO)***, 31 January 2006 (Not Releasable)

CJCSI 5250.01, ***Special Access Program (SAP) Policy***, 15 February 2007 (Resticted)

Joint Air Force-Army-Navy (JAFAN) 6/0 Manual, ***Special Access Program Security Manual,*** 29 May 2008

Joint Air Force-Army-Navy (JAFAN) 6/3 Manual, ***Protecting Special Access Program Information Within Information Systems,*** 15 October 2004

Joint Air Force-Army-Navy (JAFAN) 6/4 Manual, ***Special Access Program Tier Review Process,*** 9 May 2006

Joint Air Force-Army-Navy (JAFAN) 6/9 Manual, ***Physical Security Standards for Special Access Program Facilities,*** 23 March 2004

N-NC SAPCON Security Standard Operating Procedures (SOP), 15 December 2011

Prescribed Forms

SAP Form 6, ***Notification of Foreign Travel***

SAP Form 17, ***Record of Annual Training***

Standard Form 86, ***Questionnaire for National Security Positions***

SF-86C, ***Standard Form 86 Certification***

Abbreviations and Acronyms

AIS—Automated Information Systems

ATO—Authority to Operate

CI—Counter Intelligence

CJCS—Chairman Joint Chiefs of Staff

CPI—Critical Protected Information

DAA—Designated Approving Authority

DCADS—Defense Common Access Database System

DOD—Department of Defense

GSSO—Government SAP Security Officer

ISSP—Information System Security Plan

JWICS—Joint Worldwide Intelligence Communication System

MUA—Military Utility Assessment

NIPR—Non-Secure Internet Protocol Router

NTK—Need-to-Know

OSD—Offices of the Secretary of Defense

PL—Protection Level

PAR—Program Access Request

PM—Program Manager

PMR—Program Management Review

PSM—Program Security Manager

SAP—Special Access Program

SAP EXCOM—SAP Executive Committee

SAPF—SAP Facility

SAPCO—Special Access Program Control Office

SAPCON—Special Access Program Control Officer

SAPSM—Special Access Program Security Manager

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facility

SIPR—Secure Internet Protocol Router

SME—Subject Matter Expert

SOP—Standard Operating Procedures

STE—Secure Terminal Equipment

STO—Special Technical Operations

STOWG—STO Working Group

TSWA—Temporary Secure Working Area

UCP—Unified Command Plan

VTC—Video Teleconferences