BY ORDER OF THE
SUPERINTENDENT

HQ UNITED STATES AIR FORCE
ACADEMY INSTRUCTION 14-403

11 MARCH 2022

Intelligence

AF CYBERWORX

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-publishing.af.mil**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ USAFA/DFQI

Certified by: HQ USAFA/DFQI
(Lt Col Dressler)
Pages: 14

This publication implements Air Force Manual 14-403, *Sensitive Compartmented Information Security and Intelligence, Surveillance and Reconnaissance Systems Cybersecurity and Governance*. It is consistent with Department of Defense Manual (DoDM) 5220.22, *National Industrial Security Program: Industrial Security Procedures for Government Activities, Operating Manual*, DoDM 5105.21, Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*, DoDM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*, DoDM 5105.21, Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities*, *Intelligence Community Directive* (ICD) 121, *Managing the Intelligence Community Information Environment*, ICD 500, *Director of National Intelligence Chief Information Officer*, ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, ICD 502, *Integrated Defense of the Intelligence Community Information Environment*, ICD 503, *Intelligence Community Information Technology Systems Security Risk Management*, Certification and Accreditation, ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information* (SCI), ICD 705, *Sensitive Compartmented Information Facilities*, ICD 710, *Classification Management and Control Markings System*, ICD 731, *Supply Chain Risk Management.* This publication applies to all USAFA civilian employees and uniformed members of the US Space Force, Regular Air Force, Air Force Reserve, and Air National Guard, including contractors when included in the terms of their contracts, who supports Air Force intelligence missions at USAFA. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using Air Force (AF) Form 847, *Recommendation for Change of Publication*. The authorities to waive requirements in this publication are identified with a Tier (T-0, T-1, T-2, T-3) number following the compliance statement. See DAFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority. The waiver authority for non-tiered requirements in this publication is USAFA/DFQI. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

CHAPTER 1

AUTHORITY AND SCOPE

1.1. Purpose. This manual provides guidance regarding the governance, management, security, use and dissemination of sensitive compartmented information including the scheduling for polygraph testing.

1.2. Authority. Executive Order 12958 “Classified National Security Information,” provides the basis for classifying and controlling national security information. This document articulates the need to safeguard classified SCI information and the obligation to protect its value in the interest of national defense. This manual incorporates the provisions of applicable Federal Statutes, Executive Orders, National Directives, DoD Directives, and DoD 5-5105-21-M-1, (Reference C). This manual is promulgated pursuant to authorities and responsibilities assigned to the Director of National Intelligence and Defense Intelligence Agency (DIA) for the protection of SCI.

1.3. Scope. This manual applies to USAFA SCI programs program participants.

1.4. Program Management. United States Space Force/Space Operation Center/S2 is the USAFA SCI program Cognizant Security Office

CHAPTER 2

ROLES AND RESPONSIBILITIES

2.1. Roles and Responsibilities.

2.1.1. Director AF CyberWorx or Designated Representative:

2.1.1.1. Appoints the Primary and Alternate Special Security Representative (SSR).

2.1.1.2. Appoints the Primary and Alternate Information Security System Officer (ISSO) and Information Security System Manager (ISSM).

2.1.1.3. Approves need-to-know for individuals requiring SCI access.

2.1.1.4. Designate SCI couriers in writing, for hand-carrying SCI in the Colorado Springs Area bases.

2.1.1.5. Validates the need for SCIFs and establishment of co-utilization agreements for Special Access Programs (SAPs).

2.1.2. USAFA Commanders, Directors or Designated Representative:

2.1.2.1. Nominate USAFA military, civilians and cadets for SCI access and/or polygraph testing.

2.1.2.2. Evaluate nomination request and personnel information.

2.1.2.3. Coordinate with internal staff to resolve outstanding issue with SCI nomination.

2.1.2.4. Report any incident or derogatory information that affects personnel access to national security information to:

2.1.3. Associate Dean of Research:

2.1.3.1. Approves and coordinates annual Cadet Summer Research (CSRP) polygraph slots with Headquarters Air Force Office of Investigation (HQ AFOSI).

2.1.4. Directorate/CSRP Coordinators:

2.1.4.1. Validate nominees need to know, appropriate security clearance and non-disclosure agreement.

2.1.4.2. Submits personnel or cadet security clearance upgrade request to their unit security assistant, squadron Air Military Trainer (AMT) and courtesy copy HQ USAFA/IP.

2.1.4.3. Initiate SCI nomination process with the USAFA SSR.

2.1.5. HQ USAFA Information Protection (HQ USAFA/IP):

2.1.5.1. Review and validate Personnel Security Investigation (PSI) submission.

2.1.5.2. Coordinate with unit security assistant/AMT on PSI security questionnaire accuracy and completeness.

2.1.5.3. Submit PSI to Defense Counter-Intelligence Security Agency (DCSA).

2.1.5.4. Notify commanders/directors and the SSR of any Request for Action (RFA), Supplemental Information Request or Continuous Evaluation Alerts.

2.1.6. USAFA Unit Security Assistants/AMTs:

2.1.6.1. Validate nominees need to know, appropriate security clearance and non-disclosure agreement.

2.1.6.2. Initiate SCI nomination process with the SSR.

2.1.6.3. Initiate and process PSI and SCI-Pre Screen Questionnaire documents.

2.1.6.4. Review Electronic Questionnaires for Investigations Processing (e-QIP) and SCI-Prescreen for accuracy, completeness and positive response against the Department of Defense Central Adjudication Facility (DoD-CAF) thirteen adjudication guidelines.

2.1.6.5. Resolve any missing or incorrect information including negative data or answers with the applicant.

2.1.6.6. Recommend SCI nomination to owning commander, director or designee.

2.1.6.7. Submit PSI to HQ USAFA/IP office.

2.1.6.8. Monitor Defense Information System for Security (DISS).

2.1.6.9. Implement personnel security continuous evaluation.

2.1.7. USAFA Special Security Representative (SSR):

2.1.7.1. Manages SCI security program and SCIF day-to-day operation.

2.1.7.2. Serves as the USAFA subject matter expert for Personnel, Information, Physical, and Industrial Security relating to SCI.

2.1.7.3. Reports SCI programmatic issues to USSF/SSO, ACC/CISO and Director of CyberWorx.

2.1.7.4. Reviews and process SCI nominations, SCI Pre-Screens and e-QIP.

2.1.7.5. Validates USAFA, DoD, Federal Government and Industry SCIF or SCI visit request.

2.1.7.6. Monitors SCIF Information, telephonic systems and service availability.

2.1.7.7. Assist the Information Technology Specialist in coordinating with USSF/AF Joint Worldwide Intelligence Communication System (JWICS) Front Range Support, Air Combat Command (ACC) Chief Information Security Officer (CISO) and AF JWICS Enterprise Service Desk (ESD) for AF JWICS classified system maintenance.

2.1.7.8. Facilitates SCI initial indoctrination and security termination briefing.

2.1.7.9. Implements personnel security continuous evaluation.

2.1.7.10. Designated as Site Security Manager for USAFA SCI related construction and modification.

2.1.7.11. Appointed as Alternate Communication Security (COMSEC) custodian and Secure Voice custodian.

2.1.7.12. Coordinates with USAFA stakeholders on all security matters affecting AF CyberWorx mission.

2.1.7.13. Program SCIF information technology replacement actions.

2.1.7.14. Approve equipment procurement against Supply Risk Management concerns for information technology software and hardware in accordance Intelligence Community, DoD and supplemental policy.

2.1.7.15. Responsible for development and submission of programming and budgeting requests for SCIF facilities, sustainment, equipment and operations.

2.1.7.16. Act as the ISSM.

2.1.7.17. Develops local SCI training materials, concept, construction security, CyberWorx policy and Standard Operating Procedures.

2.1.7.18. Provides SCI initial and annual training.

2.1.8. AF CyberWorx Information Technology Specialist:

2.1.8.1. Responsible for the overall procurement, development, integration, modification, or operation and maintenance of AF CyberWorx systems.

2.1.8.2. Plan for security control implementation, assessment, and sustainment throughout the system life cycle.

2.1.8.3. Ensure authorized users and support personnel receive appropriate cybersecurity Training.

2.1.8.4. Responsible for the IT's cybersecurity program within a program, organization, information system, or enclave.

2.1.8.5. Develop and maintain an organizational or system-level cybersecurity program.

2.1.8.6. Maintain awareness of program's cybersecurity risk posture based on current threats.

2.1.8.7. Reports incidents to the Authoring Official and appropriate reporting chains and coordinating system level responses to unauthorized disclosures.

2.1.8.8. Manages Computer Security (COMPUSEC), Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) and Communications Security (COMSEC) Operations.

2.1.8.9. Ensure cybersecurity inspections, tests, and reviews are coordinated with leadership as necessary.

2.1.8.10. Report security violations and cybersecurity incidents to Authorizing Officials (AO) according to their reporting procedures and criteria.

2.1.8.11. Manage all software licenses owned by the organization in support of the base software license management program.

2.1.8.12. Coordinates AF JWICS system services and maintenance with USSF/AF Joint Worldwide Intelligence Communication System (JWICS) Front Range Support, Air Combat Command (ACC) Chief Information Security Officer (CISO) and AF JWICS Enterprise Service Desk (ESD).

2.1.8.13. Orchestrates NIPR, SIPR and Mission Net services and maintenance with 10th Communication Squadron.

2.1.8.14. Designated as AF CyberWorx system ISSO or ISSM.

CHAPTER 3

PERSONNEL SECURITY

3.1. SECURITY CLEARANCES AND ACCESS.

3.1.1. Nomination:

3.1.1.1. USAFA Commanders, Directors or Designated Representative can nominate personnel for SCI access in accordance with validated mission need. (T-3)

3.1.1.2. Nominating official must confer with their unit security assistant to ensure nominee meets the minimum access eligibility requirement and there are no pending unfavorable administrative actions. (T-3)

3.1.2. Eligibility Determinations:

3.1.2.1. Nominees must have an in scope T5 or T5R investigation with an Eligibility Level of SCI - ICD704 reflected in DISS. (T-0)

3.1.2.2. Interim SCI request must have a completed interim Top Secret case adjudicated by the Commander or Director and reflected on DISS prior to submitting access request to DoD CAF. (T-0)

3.1.2.3. Sponsoring squadron, directorate or agency is responsible for coordinating required security clearance upgrade with HQ USAFA/IP. (T-3)

3.2.1. Polygraph Scheduling:

3.2.1.1. PCS polygraph needs must be validated through Air Force Personnel Center (AFPC) Personnel Processing Code (PPC) prior to scheduling. (T-1)

3.2.1.2. CSRP polygraph annual slots are identified via CSRP Directorate representative. (T-3)

3.3.1. Visit Request:

3.3.1.1. The SSR is the official channel for submitting SCI access certification. (T-3)

3.3.1.2. Requesting personnel are responsible for sending DISS Visit Authorization Request (VAR) five duty days prior to visit start and confirm receipt with the SSR.

3.3.1.3. USSF Special Security Officer (SSO) will certify foreign national personnel SCI equivalent clearance prior to visit. (T-1)

3.4.1. Reporting:

3.4.1.1. Personnel must report any changes in status with their supervisor, unit security assistant, SSR and HQ USAFA/IP in accordance with SEAD 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position.* (T-1)

CHAPTER 4

INFORMATION SECURITY

4.1. INFORMATION ASSURANCE AND PROTECTION.

4.1.1. SCI material storage is only in approved SCIF. (T-0)

4.1.2. Destruction of SCI materials is only permitted in the SCIF. (T-0)

4.1.3. SCI information outside the SCIF is only allowed via designated SCI COURIER in the Colorado Springs Area bases. (T-2)

4.1.3.1. There is a USAFA courier limit of 75 mile radius. (T-2)

4.1.4. Access to SCI Computers, VOIP, VTC and DVTC is in accordance with appropriate clearance, need to know and signed Non-disclosure Agreement (NdA). (T-0)

4.1.4.1. AF JWICS Account Request include:

4.1.4.1.1. DD Form 2875, *System Authorization Access Request (SAAR).* (T-1)

4.1.4.1.2. AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision.* (T-1)

4.1.4.1.3. *Air Force JWICS User Agreement and KVM Agreement.* (T-1)

4.1.5. Non-SCI meetings or access to collateral systems (SIPRNET, SVTC or Viper phones) in the SCIF will be approved by the AF CyberWorx director.

4.1.6. All request must be submitted via AF CyberWorx scheduling system.

4.1.7. USSF SSO will certify SCI information access of foreign nationals prior to visit. (T-1)

CHAPTER 5

PHYSICAL SECURITY

5.1. ACCESS CONTROL.

5.1.1. Access to the AF CyberWorx facility is coordinated through the SSR or designated representative by the visit Action Officer or security assistant through DISS SMO code SSR USAFA-1.

5.1.1.1. Personnel with SSO/SSR submitted SCI Visit Access Request (VAR) on file or verified security clearance via DISS or Scattered Castle and completed SOP training will not require an escort. (T-1)

5.1.1.2. All other access requires escorts at all times. (T-1)

5.1.1.3. All requests must be submitted via AF CyberWorx scheduling system.

5.1.2. USSF SSO will certify physical security access of foreign nationals to USAFA sensitive compartmented information facilities prior to visit. (T-1)

CHAPTER 6

INDUSTRIAL SECURITY

6.1. CONTRACT MANAGEMENT.

6.1.1. Contracts with SCI components must be coordinated and approved through the sponsoring SSO or SCI Cognizant Security Office. (T-1)

6.1.2. Contractor access to USAFA SCIF is coordinated by the government contract owner or representative. (T-3)

CHAPTER 7

TRAINING

7.1. TRAINING REQUIREMENTS. All personnel, regardless of classified access or security clearance eligibility must receive initial orientation. Those members granted access to classified information must receive initial orientation and annual refresher training.

7.1.1. Cadets who access SCI information on a routine basis and associated classified information system (i.e. AF JWICS), require more extensive training.

7.1.1.1. Cadets will complete the following training located at **https://securityawareness.usalearning.gov/index.html**. Cadets will submit their certificate to **SSR_USAFA@usafa.edu** (or successor system). (T-3)

7.1.1.1.1. Counterintelligence Awareness and Reporting Course for DOD. (T-3)

7.1.1.1.2. Derivative Classification. (T-3)

7.1.1.1.3. DoD Mandatory Controlled Unclassified Information (CUI) Training. (T-3)

7.1.1.1.4. Insider Threat Awareness. (T-3)

7.1.1.1.5. Unauthorized Disclosure of Classified Information andControlled Unclassified Information. (T-3)

7.1.1.1.6. OPSECAwarenessfor Military Members, DOD Employees and Contractors. (T-3)

7.1.2. Polygraph candidate are required to complete the following training provided by the SSR and acknowledge completion via email to **SSR_USAFA@usafa.edu** (or successor system).

7.1.2.1. Security Executive Agent Directive (SEAD) Information. (T-3)

7.1.2.2. SEAD Reporting. (T-1)

7.1.3. AF JWICS Account Request requires the following training to be completed and documents sent to **SSR_USAFA@usafa.edu** (or successor system). Training can be accomplished via My eLearning. **NOTE:** SCI Program access required.

7.1.3.1. Cyber Awareness Challenge. (T-1)

7.1.3.2. Derivative classification. (T-1)

7.1.3.3. NATO Training.

7.1.3.4. Standard Operating Procedure (SOP). (T-3) **NOTE**: Provided during initial account access.

7.1.4. Annual SCI Security Education and Awareness Training (SETA) program is applicable to personnel with SCI access. Training can be accomplished via My eLearning.

7.1.4.1. Derivative Classification Refresher (Bi-Annually). (T-3)

7.1.4.2. SCI Refresher (Annual). (T-1)

CHRISTOPHER McCLERNON, Colonel, USAF
HQ USAFA/DFQ

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFMAN 14-403, *Sensitive Compartmented Information Facility and Intelligence, Surveillance and Reconnaissance Systems Cybersecurity and Governance*, 2 September 2019

AFPD 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise,* 11 July 2019

AFI 16-1402, *Insider Threat Program Management,* 16 Jul 2020

AFI 16-1406, Volume 2, *Air Force Industrial Security Program*, 25 August 2020

AFI 33-360, *Publication and Forms Management,* 1 December 2015

AFI 33-322, *Records Management and Information Governance Program,* 27 July 2021

AFI 63-101_20-101, *Integrated Life Cycle Management*, 29 June 2020

AFOSI 71-103V1, *Air Force Polygraph Program,* 9 May 2019

DoDM 5220.22, *National Industrial Security Program Operating Manual,* May 18, 2016

DoDM 5105.21, Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security, Incorporating Change 2, Effective* October 6, 2020

DoDM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security, Incorporating Change 2, Effective* October 6, 2020

DoDM 5105.21, Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities, Incorporating Change 2, Effective* October 6, 2020

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT), Incorporating Change 1, Effective* October 7, 2019

ICD 121, *Managing the Intelligence Community Information Environment,* 19 January 2017

ICD 500, *Director of National Intelligence Chief Information Officer,* 7 August 2008

ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community,* 21 January 2009

ICD 502, *Integrated Defense of the Intelligence Community Information Environment,* 11 March 2011

ICD 503, *Intelligence Community Information Technology Systems Security Risk Management,* 21 July 2015

ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information (SCI),* 21 June 2013

ICD 704, *Personnel Security Standard and Procedures Governing Eligibility for Access to Sensitive Compartmented Information,* 1 October 2008

ICD 705, *Sensitive Compartmented Information Facilities,* 26 May 2010

ICD 710, *Classification Management and Control Markings System,* 21 June 2013

ICD 731, *Supply Chain Risk Management,* 7 December 2013

ICPG 704.5, *Intelligence Community Personnel Security Database Scattered Castles,* 25 February 2020

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision*

DD Form 2875, *System Authorization Access Request (SAAR)*