BY ORDER OF THE COMMANDER
374TH AIRLIFT WING

YOKOTA AIR BASE INSTRUCTION
16-1401

5 JUNE 2025

Operations

SECURITY ENTERPRISE – INFORMATION PROTECTION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 374 AW/IP

Certified by: 374 AW/IP
(GS-12 Christopher R. Turner, Sr.)
Pages: 90

This publication applies to all military, civilian and government contractor personnel assigned to, or visiting Yokota Air Base (Yokota AB), 374th Airlift Wing (AW), mission partners and those separated units assigned to the 374 AW. This instruction does not apply to AF Reserve, Air National Guard, or Civil Air Patrol personnel unless performing roles on and in support of Yokota Air Base. This publication addresses policies and procedures for implementation of AFPD 16-14, *Security Enterprise Governance*, DAFI 16-1401, *Information Protection Program*, AFI 16-1402, *Counter-Insider Threat Program Management*, DoDM5200.01_AFMAN 16-1404 (Vols 1-3), *Information Security Program*, AFI 10-701, *Operations Security (OPSEC)*, DoDM5200.02_DAFMAN 16-1405, *Department of Air Force Personnel Security Program*, and DoDM5220.22V2_AFMAN16-1406V2, *Industrial Security*. This publication outlines information protection program requirements. It prescribes appointment procedures and responsibilities for commanders and unit security managers (USMs) and minimal Top Secret Control Officer (TSCO), responsibilities. This publication does not apply to the internal application of Top Secret Sensitive Compartmented Information Facilities (SCIF). SCIF and SCI rules are governed primarily by DODM 5105.21, V 1-3, *Sensitive Compartmented Information (SCI) Administrative Security Manual*, Director of National Intelligence (DNI), Intelligence Community Directive (ICD), Intelligence Community Standard (ICS) 705 (ICD 705) and AFMAN 14-403, *Sensitive Compartmented Information Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance*. The 374 AW Special Security Officer (SSO) located in 374 OSS/IN will oversee SCI programs/facilities located on Yokota Air Base but will work in conjunction with 374 AW/IP for items not exclusively covered by SCI governance. This publication predominantly covers collateral TOP SECRET-level and below information and explains required actions regarding security violations; access, dissemination, accountability of information; transmission of information and material; disposal/destruction

procedures; and security education and training awareness (SETA) program. It also establishes the local policies and responsibilities for the oversight, management, and execution of the Yokota AB Security Enterprise (SECENT) and IP programs and is directive in nature. Compliance is mandatory for all personnel and the terms “must,” “shall,” and “will” denote mandatory actions in this instruction. The terms “should” or “may” indicate preferred, but non-mandatory actions. Failure to comply with the publication is punishable as a violation of Article 92, Uniform Code of Military Justice (UCMJ). In order to comply with this publication, the collection and maintenance of information protected by the Privacy Act of 1974 will be required. The authority to collect and maintain the records prescribed in this publication is 10 U.S.C. 8012; 44, U.S.C 3101; and EO 9397 (AF Form 2583, Request for Personnel Security Action). Authority: 10 U.S.C. 8012; 44 U.S.C 3101; and EO 9397. Principal Purposes: To outline information protection local requirements. Routine Uses: To request personnel security investigations, record emergency or limited access authorization. Social Security Number [SSN] is used for positive identification of individuals and records in regard to security investigations and access authorization to classified information. Disclosure is voluntary: Failure to provide the SSN could result in assignment to less sensitive duties or denial to access of classified information. Forms affected by the Privacy Act have the appropriate statement. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW AFI 33-322, *Records Management and Information Governance Program*, and dispose of IAW the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at https://www.my.af.mil/afrims/afrims/afrims/rims.cfm. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, Recommendation for Change of Publication; route AF Forms 847 from the field through their appropriate functional chain of command. (This publication has been reviewed in accordance with AFI 10-701, *Operations Security*).

Chapter 1
PROGRAM OVERVIEW

1.1. Air Force Security Enterprise. AFPD 16-14, *Security Enterprise Governance*, and DoDM 5200.01V1_AFMAN 16-1404 V1-3, *Information Security Program*, defines the Air Force Security Enterprise (AFSEC) as the organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard AF personnel, information, operations, resources, technologies, facilities, and assets against harm, loss, or hostile actions. This requires interagency cooperation between IP and multiple other administrative security functions to include other traditional security programs which fall under the Mission Assurance portfolio described in AFPD 16-14. The combined program at Yokota AB is called the Security Enterprise (SECENT) program and includes the IP and other security functional programs.

1.1.1. Scope of the Yokota AB Security Enterprise (SECENT). The Yokota AB SECENT focuses on administrative security functions, leaving the more traditional Security Forces (SF) functions (e.g., physical security such as gate entry, Protection Level (PL) resource protection, base defense, anti-terrorism, etc.) to the SF functions of the 374th Security Forces Squadron (SFS).

1.1.2. Information Protection is a subset of the Air Force Security Enterprise. It consists of the following core security disciplines: Personnel Security (PERSEC), Information Security (INFOSEC), and Industrial Security (INDUSEC) but also includes oversight of SECENT-associated Operations Security (OPSEC), Counter-Insider Threat (C-InT), and Security Education and Training Awareness (SETA) programs.

1.1.2.1. The 374 AW/IP office is the sole focal point on matters pertaining to the security programs managed under Information Protection.

1.1.2.2. The 374 AW/IP office reports directly to the 374 AW Deputy Commander (374 AW/CD) through the Chief, Information Protection (CIP) IAW DAFI 16-1401, paragraph 2.14.2.

1.2. Non-PACAF Tenant Unit Agreement.

1.2.1. Non-PACAF tenant units on Yokota AB (YAB) and geographically separated tenant units supported by YAB are automatically entered into 374 AW IP Program apart of a host-tenant support agreement in accordance with associated Base Support Agreement. All units with classified holdings will be inspected annually by the 374 AW/IP IAW DoDM 5200.01_AFMAN 16-1404V1, Enclosure 3, Section 19. Units/security managers utilizing the 374 AW/IP DISS parent SMO Code as a subordinate organization must meet training requirements to maintain an account.

1.2.2. Tenant units are encouraged to participate in the host base's IP Program, but a tenant unit commander may decline (opt out) of participation. If opting out, the unit commander (or equivalent) will provide a signed memorandum formally requesting exemption from participation in all or part of the 374 AW IP program. It will confirm that the unit is not participating directly in the 374 AW IP program and must receive IP program oversight from their cognizant MAJCOM, higher echelon unit and/or parent organization. This will gain exemption from the annual IP inspection requirement from the 374 AW. The memorandum will be maintained by 374 AW/IP and should be reviewed annually.

1.2.3. All IP program requirements established by PACAF and the host base Wing (374 AW), as applicable, must be complied with and adhered to by all units, regardless of whether a unit participates in the 374th Airlift Wing, Information Protection Program or not.

Chapter 2
ROLES, RESPONSIBILITIES AND TRAINING

2.1. Commander and Deputy Commander, 374th Airlift Wing.

2.1.1. The Commander, 374th Airlift Wing delegates responsibilities and oversight of the Information Protection Office to the Deputy Commander, 374th Airlift Wing for ensuring security controls, safeguards, and countermeasures are established through the application of risk management principles, as appropriate, for Yokota Air Base assigned organizations, including mission partners. The Deputy Commander, 374th Airlift Wing will enforce standards for safeguarding, storing, destroying, transmitting, transporting; and mitigate the adverse effects of unauthorized access or disclosure, compromise, or loss by inquiry or investigation and acting upon reports of security incidents and violations involving classified information, critical information, and controlled unclassified information (CUI).

2.1.1.1. Approve and recertify open storage areas (unless delegated to CIP).

2.1.1.2. Review and approve annual self-inspection reports and security classification management data reports for submittal to HQ PACAF/IP.

2.1.1.3. Establish at least one classified clean-out day per year to dispose of unneeded classified material. (Additional days may be added depending upon the availability of authorized destruction methods).

2.1.1.4. Ensure Security Incidents are reported to the Chief, Information Protection within 24-hours of discovery and inquiry/investigation reports are completed within the timelines as listed in DoDM 5200.01_DAFMAN 16-1404V3, Enclosure 6 and this instruction.

2.1.1.5. Approve security-in-depth and supplemental control determinations as required, in accordance with DoDM 5200.01_DAFMAN 16-1404V3.

2.1.1.6. Enforce requirements to complete Standard Form 85 and 86 (eAPP) for reinitiating background and security clearance investigations.

2.1.1.7. Enforce Continuous Evaluation reporting requirements as outlined in DoDM 5200.02_**D**AFMAN 16-1405, *Air Force Personnel Security Program*, Section 11.

2.2. Chief, Information Protection (CIP).

2.2.1. Executes Information Protection responsibilities on behalf of the Commander and Deputy Commander, 374th Airlift Wing and provides oversight and direction to commanders, directors, agency chiefs, security managers, assigned security specialists, and mission partners on and off the installation. Hereinafter, the term commander/director/agency chief will be referred to as "Commander."

2.2.1.1. Reports directly to the Deputy Commander, 374 Airlift Wing, who is designated supervisor in accordance with DAFI 16-1401, *Information Protection Program*.

2.2.1.2. Implements and monitors the Information Security Program, Personnel Security Program, Industrial Security Program, Operations Security Program, Counter-Insider Threat Program, Security Education & Training Awareness Program and the Mission Partner Identity, Credential and Awareness Management (MP-ICAM) Program.

2.2.1.3. Appointed as the Installation Security Manager and may perform security manager functions for small units not requiring an assigned security manager (including mission partner and geographically separated units) or during the absence of designated unit security managers. Personnel permanently assigned to the Wing Information Protection office may also perform the Installation Security Manager functions.

2.2.1.4. Prepares the annual Information Security Oversight Office (ISOO) Report for the Deputy Commander, 374th Airlift Wing to review for submission to HQ PACAF/IP.

2.2.1.5. Prioritizes and balances office workload depending upon need of each program.

2.2.1.6. Trains security managers on their duties and responsibilities in accordance with DoDM 5200.01_DAFMAN 16-1404V3, Enclosure 5. Will remove security managers' access to the Defense Information System for Security (DISS) if a security manager fails to maintain the proper clearance, complete the SF 86, *Questionnaire for National Security Positions*, within timelines for a reinvestigation, or fails to attend annual training without a valid reason. The Chief, Information Protection (CIP) will determine if the reasons for missing training are valid.

2.2.1.7. Reviews approval/recertification packages (includes coordination with SFS, CES, and Wing Cybersecurity) for open storage areas (OSA) to be approved by the Deputy Commander, 374th Airlift Wing or CIP (if delegated).

2.2.1.8. Must consult on proposed construction projects for new classified holding areas during each design phase of the project. 374 CES or applicable lead agency will ensure the CIP is part of the design and submittal phase.

2.2.1.9. Must consult on renovation projects for open storage areas prior to any construction implementation and will develop a recertification package for approval by the Deputy Commander, 374th Airlift Wing or CIP, after construction has been completed.

2.2.1.10. Provides advice and assistance to commanders and unit personnel on security matters and recommends improvement measures. All Information Protection (IP) security-related questions should be through the Wing IP.

2.2.1.11. Work with units to develop necessary standard operating procedures (SOPSs) to protect classified information.

2.2.1.12. Ensures training requirements, as listed in this instruction are conducted and documented.

2.2.1.13. Reviews and processes challenges to classification decisions and notifies originators of improperly marked classified documents. Informal challenges will be handled by the unit with the inquiry. Formal challenges will follow the procedures as outlined in DoDM 5200.01V1_ AFMAN 16-1404V1, Enclosure 4, Section 22 and be handled by the 374 AW/IP. The Deputy Commander, 374th Airlift Wing will be notified by the CIP prior to formal challenges initiation (due to all OCAs being General Officers/SES).

2.2.1.14. Verifies Security Incidents and Classified Message Incidents (CMI), works with the unit commander and USMs to initiate security incidents, monitors preliminary inquiries and formal investigations of security incidents for sufficiency and timeliness in accordance with DoDM 5200.01V3_ AFMAN 16-1404V3, Enclosure 6. Notifies 374 AW/CD (374

AW/CC during absence) of security incidents within 24-hours or if inappropriate actions are taken by commanders to correct deficiencies or close security incidents. When subsequent inquiries or investigations indicate no incident occurred, the owning unit commander may terminate the process. Depending on the circumstances, formal appointment of an inquiry official may not be warranted. An inadvertent infraction where an informal inquiry could prove beyond a doubt there was no compromise or loss of classified information may be closed by an informal inquiry Memorandum for Record (MFR) signed by the commander. However, details of the incident, outlining required information as if a formal investigation must be listed within the MFR for tracking purposes and HHQ reporting. If determined appropriate, the MFR would alleviate the need to conduct a formal inquiry, which requires an appointment letter, inquiry report, technical review, and closure memorandum.

2.2.1.15. Manages the Defense Information Systems for Security (DISS) program and ensures security clearance data is effectively and accurately tracked.

2.2.1.16. Directs unit personnel to complete security clearance investigations and periodic reinvestigations, as required. Coordinates with commanders and USMs to ensure clearances are completed within required timelines.

2.2.1.17. Assists units with developing emergency plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of compromise. A copy of emergency plans will be posted inside the inner door of each OSA or classified processing area (CPA). See **Attachment 2**, 374 AW Emergency Protection, Removal and Destruction of Classified Material Template.

2.2.1.18. Coordinates on behalf of the Deputy Commander, 374th Airlift Wing, at least one classified clean-out day per year to dispose of unneeded classified material. (Additional days may be added depending upon the availability of authorized destruction methods). Reports the number of classified materials destroyed with a memorandum for record during the annual report.

2.2.1.19. Conducts unit staff assistance visits when requested by commanders or primary security managers.

2.2.1.20. Reviews unit requested residential storage packages for the Deputy Commander, 374th Airlift Wing concurrence prior to the forwarding to HQ PACAF/IP for approval.

2.2.1.21. Develops and provides training material for Controlled Unclassified Information (CUI) created, handled, stored or destroyed on the installation.

2.2.1.22. Maintains the capability within the office to destroy small amounts of SECRET-level and below paper products and compact disks with approved shredders.

2.2.1.23. Conducts periodic inspections of the Base Recycle Center and Incinerator to ensure controlled/marked documents are being shredded and not thrown in the trash.

2.2.1.24. Develops and maintains current listing of commander appointed and Wing IP trained unit security managers for use by the Pass and Registration Office and Cybersecurity Liaison personnel to verify authorization to sign documents verifying security clearances and background checks.

2.2.1.25. Coordinate and sign Industrial Contractor Agreement Letters and Memorandums with contract companies assigned to work with classified information once the DD Form 254 has been properly coordinated and signed by all respective parties IAW DoDM 5220.22V2_ AFMAN 16-1406V2, *National Industrial Security Program*.

2.3. Commanders.

2.3.1. Responsible for ensuring a viable Information Protection program within their units.

2.3.1.1. Appoints in writing a primary and alternate unit security manager with a minimum of a SECRET Security Clearance for a period no less than one year due to training and learning requirements. Security managers will have unfettered access to the commander due to time deadlines for processing security-associated paperwork to the requesting Defense Counterintelligence and Security Agency Adjudication and Vetting Services (DCSA AVS). Responses to DCSA AVS in many cases are limited to ten days and could affect a member's security clearance eligibility if not answered by a given deadline. Responses to DCSA AVS WILL NOT be staffed through the security manager's chain-of-command lower than the commander. Security clearances removed by DCSA AVS for failure to meet timelines take 12-24 months to regain access and correct. Contractor personnel will not be appointed as USMs.

2.3.1.2. Appoints in writing at least one security container, open storage area, and/or Secret Internet Protocol Router Network (SIPRNET) lockbox custodian(s). Custodians are responsible for taking care of the security container (i.e. safe). Other members requiring the combination to one of the items/areas noted above do not have to be on the custodian letter.

2.3.1.3. Initiates Security Information File (SIF) on assigned personnel as required by DODM 5200.02_DAFMAN 16-1405, *Procedures for the DoD Personnel Security Program*, Continuous Evaluation Program, Section 11, CE Reporting Requirements as outlined.

2.3.1.4. Grants personnel access to classified information in DISS and continually evaluates their trustworthiness IAW DoDM 5200.02_DAFMAN 16-1405. The USM will make entries into DISS on behalf of the unit commander granting level of access consistent with SAR codes as listed on the Unit Manning Document.

2.3.1.5. Ensures all unit personnel are aware of their responsibilities when handling, controlling, or possessing classified information/materials. In accordance with DoDM 5200.01V3_DAFMAN16-1404V3. Everyone, who works with classified information is ***personally responsible*** for taking proper precautions to ensure that unauthorized persons do not gain access to classified information.

2.3.1.6. Implements an ongoing security education and training program ensuring annual training is provided to all members of the organization.

2.3.1.7. Commanders will ensure a tracking mechanism documenting completion of initial and recurring training to show type of training, rank, name, and date training was completed. Training materials are available on the 374 AW/IP SharePoint website.

2.3.1.8. Immediately appoint in writing an Inquiry Official (IO) in a rank/grade equal to, or higher of than the suspected culpable parties involved in the incident. Ensure the IO completes the inquiry and written report within 10-duty days IAW DoDM 5200.01V3_D

AFMAN 16-1404V3, Enclosure 6 unless an informal inquiry MFR is appropriate (see previous paragraph 2.2.1.13).

2.3.1.9. Reviews security incident reports and determines final disposition based on IO report and 374 AW/IP technical review/recommendations IAW timelines in paragraph 11.2 of this instruction.

2.3.1.10. Ensures unit Emergency Plans are developed for areas processing or handling classified information.

2.3.1.11. Approves classified meetings and conferences by appointing an individual to conduct preparation requirements IAW the Classified Meeting Checklist, see **Attachment 3**. Classified briefings or conferences will not take place outside a U.S. Government owned facility unless an exception is approved in advance by SAF/AA. Organizations/information owners conducting classified meetings, briefings, conferences, seminars, workshops, etc., are responsible for ensuring only cleared personnel are in attendance and the Classified Conference Meeting Checklist items are complied with. The Information Protection Office can provide guidance if needed on completing the checklist or conducting these briefings.

2.3.1.12. Take corrective actions to address areas identified by the 374 AW/IP inspection reports.

2.3.1.13. Ensure the 374 AW/IP is listed on each unit's in and out-processing checklist and each assigned individual (military, US civilian, and DOD contractor) immediately process through their respective USM to ensure security clearances remain current and valid in DISS. (The DCSA AVS will withdraw or revoke personnel's security clearance who fail to in-process their respective unit or 374 AW/IP due to lacking an owning organization).

2.3.1.14. Ensure USMs comply with responsibilities as outlined in this instruction.

2.3.1.15. Establish a system to conduct end-of-day security checks using the SF 701, *Activity Security Checklist*; the SF 701s are used for vaults, safes, and open storage areas and will be maintained for the current month unless required longer by specific programs. The SF 701 is not required for 24/7 work centers, however, it is highly recommended to complete the SF 701, at a set time, once every 24-hours to ensure security of the area is being maintained.

2.3.1.16. Ensure personnel use the SF 702, *Security Container Check Sheet*, to record each opening, closing, and checking of vaults, security containers, safes and open storage areas. If a security container or OSA has not been opened the "*Checked By*" column must still be annotated. Completed SF 702s will be maintained for the current month unless required longer for specific programs.

2.3.1.17. Continuously monitor and evaluate personnel with clearances for indicators that may signal matters of personal concern that could potentially affect National Security IAW DoDM 5200.02._AFMAN 16-1605, Section 11: Continuous Evaluation and Reporting Requirements.

2.3.1.18. Review and validate unit's manning billets attributes within Manpower Programming and Execution System (MPES) annually by 15 May in accordance with

DoDM 5200.02_DAFMAN 16-1405, Section 2, para 2.13(i)(2).

2.4. Unit Security Manager(s) (USM).

2.4.1. The USM(s) are responsible for implementing and managing the PERSEC, INFOSEC, and INDUSEC programs as well as provide coordination of SECENT-associated OPSEC, C-InT, and SETA programs on behalf of the unit commander.

2.4.2. Unit Security Managers will be appointed in writing by their respective commander due to granting access to unit members PII; see **Attachment 4**. USMs not appointed in writing will not be given access to DISS and cannot sign DD Form 2875 for access to the network or information systems programs or AF Form 2586 for the issuance of a Restricted Area Badge (RAB); appointment letters will be sent electronically to the 374 AW/IP. Unit security managers must complete required training and attend quarterly USM meeting with Wing IP or will be recommended for removal from the SECENT program.

2.4.3. Criteria to be appointed as a USMs:

2.4.3.1. Personnel must possess a minimum of a Secret Security Clearance in order to be granted access to DISS.

2.4.3.2. Personnel must be in the grade of E-5/civilian equivalent or above for primary USMs.

2.4.3.3. Assistant/alternate USMs must be in the grade of E-4/civilian equivalent or above.

2.4.3.4. Personnel must have at least one-year retainability due to training requirements, account access and level of knowledge required to manage the unit program.

2.4.3.5. New USMs will sign up for a Security Training, Education and Professionalization Portal (STEPP) account located at the following link

https://cdse.usalearning.gov/login/index.php. Prior to attending the 374 AW/IP Initial Unit Security Managers training, the following DCSA CDSE course must be completed as prerequisite and the USM must provide a copy of the certificate to the 374 AW/IP:

Air Force Security Manager Program (GS100.CU) (13 hours);

https://www.cdse.edu/Training/Curricula/GS100/

2.4.3.6. The 374 AW/IP will conduct initial unit security manager training (quarterly) for all newly appointed security managers prior to granting access to DISS.

2.4.3.7. Complete training requirements IAW DoDM 5200.01V3_AFMAN 16-1404V3, Enclosure 5.

2.4.4. USMs will execute following actions:

2.4.4.1. Ensure initial orientation and annual refresher training is conducted for all unit cleared or uncleared personnel assigned and tracked by name, rank, and date trained IAW DoDM 5200.01V3_AFMAN 16-1404. Initial/annual training slides are located on the 374 AW/IP SharePoint website.

2.4.4.2. Ensure all unit personnel are aware of their responsibilities when handling, controlling, or possessing classified information/materials. In accordance with DoDM 5200.01V3_DAFMAN 16-1404V3, everyone, who works with classified information is ***personally responsible*** for taking proper precautions to ensure that unauthorized persons

do not gain access to classified information.

2.4.4.3. Ensure personnel who request access possess a valid security clearance prior to granting access IAW DoDM 5200.01V3 AFMAN 16-1404, Enclosure 2. Entry Authority List (EAL) or DISS visit request with clearances listed may be used to verify clearances. The 374 AW/IP or unit security managers may verify clearances in DISS verbally over the phone when EAL or visit request are not immediately available. Personnel who have not had their clearance verified will not be granted access to classified areas, information, or to perform duties handling classified information regardless of rank or position.

2.4.4.4. Use DISS to update assigned personnel's classified information access level, address DCSA AVS notifications, and modify unit personnel's profile and status such as in and out process members.

2.4.4.5. Ensure required unit personnel complete the SF 312, *Classified Information Nondisclosure Agreement*, update the date of completion, submit the signed document in DISS, and forward the completed form to the Wing Information Protection for final mailing to the correct location. Digital signatures on the SF 312 are allowed as well as wet signature.

2.4.4.6. USMs are responsible for accomplishing tasks and duties in coordination with the Wing Information Protection office.

2.4.4.7. Notify 374th AW/IP of security incidents within 24-hours and coordinate required actions with the unit commander IAW paragraph 11.2.

2.4.4.8. Ensure 374 AW/IP has a list of all classified security containers and SIPRNET lock boxes held by your unit.

2.4.4.9. Notify 374 AW/IP when areas/rooms are being considered for OSA, CPA or classified vaults to be placed into service or when new facilities will be designed containing one of these type areas.

2.4.4.10. Responsible for ensuring security-in-depth exist for areas containing classified information and systems.

2.4.4.11. Update assigned personnel access level to classified information in DISS. Monitor and act on DISS notifications. Use DISS to in-process new unit members and out-process personnel departing the unit. This applies to active duty, civilians, contractors, volunteers, and any other personnel assigned or working for the organization requiring access to classified information. Contractors will be members of the assigned unit just as military and civilian members and will participate in all applicable IP programs.

2.4.4.12. Verify prior to access being granted to classified information systems or assignment as derivative classifiers, personnel complete initial security training and annual training every 12-months thereafter. Track completion of training to show type of training, name of individual trained, rank, and date training was completed.

2.4.4.13. Ensure all unit personnel are aware of their responsibilities when handling, controlling, or possessing classified information/materials. In accordance with DoDM 5200.01V3_DAFMAN 16-1404V3. Everyone, who works with classified information is ***personally responsible*** for taking proper precautions to ensure that unauthorized persons do not gain access to classified information. Personnel requesting access must have their

security clearance verified prior to granting access IAW DoDM 5200.01V3_AFMAN 16-1404V3, Enclosure 2. Entry Authority List (EALs) or DISS visit request with clearances listed may be used to verify clearances. The 374 AW/IP staff or unit security managers may verify clearances in DISS verbally over the phone when EALs or visit request are not immediately available. Personnel who have not had their clearance verified will not be granted access to classified areas, information, or to perform duties regardless of rank or position.

2.4.4.14. Assist in the development of residential storage packages when needed by a member of the unit with assistance of 374 AW/IP. Residential storage will be reserved for those members in the grade of O-6 and above unless approved in writing by the Commander, 374th Airlift Wing.

2.4.5. USM(s) will maintain a continuity book or electronic folder containing the following items, which are subject to inspection.

2.4.5.1. Unit Security Manager Appointment Letter.

2.4.5.2. Unit Security Manager Training Certificate from 374 AW/IP.

2.4.5.3. Most recent Annual IP Inspection Report completed by 374 AW/IP. Also, a copy of corrective actions memorandum if discrepancies were found.

2.4.5.4. Listing of individuals designated in writing by the commander as derivative classifiers.

2.4.5.5. Listing of all mandatory annual security training which includes rank, name, training title/topic, and date completed of all assigned unit personnel. Everyone requires annual refresher training as well.

2.4.5.6. Most current classified information annual clean-out day results.

2.4.5.7. Most current copy of Manpower Programming and Execution System (MPES) annual billet review memorandum.

2.5. All Yokota AB Personnel Responsibilities.

2.5.1. In accordance with DoDM 5200.01V3_DAFMAN 16-1404V3. Everyone, who works with classified information is ***personally responsible*** for taking proper precautions to ensure that unauthorized persons do not gain access to classified information. Each individual authorized access to any type of sensitive information (i.e., classified or CUI), regardless of the format (i.e., electronic, hardcopy, etc.), is responsible to comply with implementing DoD/AF guidance and this instruction. This includes understanding individual responsibilities for properly protecting classified information and CUI under their custody and control. Personnel (including assigned contractor personnel) must understand ANY sensitive information may be of value to our adversaries and must be properly protected, which requires:

2.5.1.1. Marking Sensitive Information Correctly. Each individual must handle, mark, and properly control access to sensitive information entrusted to their care. This requires changing the common mindset of “only classified information" is important and also enforce CUI safeguards, markings and controls.

2.5.1.2. Maintaining Positive Control. Each individual must verify sensitive information under their control is properly protected when not under positive control. Positive control

may be as simple as locking a computer before leaving for lunch to protect CUI or as complicated as performing closure actions to secure an alarmed area where classified information is stored.

2.5.1.3. Positive control also means never cutting corners on safeguarding sensitive information, regardless of classification, category or type.

2.5.1.4. It is critical to understand our adversaries often collect CUI as a primary source of indicators for classified operations and criminals attempt to collect personal identifiable information (PII) to engage in identity theft.

2.5.1.5. Protective measures established for protecting sensitive information are gauged on the identified risk for the specified type/category of information. Failing to use the required protective standards makes the information more susceptible to adversarial collection and exploitation.

2.5.1.6. Be constantly alert to detect and report unauthorized attempts to access sensitive information at any level.

2.5.1.7. Continually monitor and evaluate personnel with clearances for indicators that may signal matters of personal concern that could potentially affect National Security IAW DoDM 5200.02_DAFMAN 16-1405, Section 11: *Continuous Evaluation and Reporting Requirements.* Report to the unit commander any conduct or information that may affect a person's trustworthiness, reliability, or loyalty (i.e., drug use, alcohol abuse, excessive indebtedness, criminal conduct/arrest, etc.).

2.5.1.8. Report to their unit commander any conduct or information that may affect a person's trustworthiness, reliability, or loyalty IAW the National Security Adjudicative Guidelines (i.e., drug use, alcohol abuse, excessive indebtedness, criminal conduct/arrest, etc.).

2.5.1.9. Ensure security taskings (i.e., end-of-day security checks) are conducted correctly, timely and annotated as required.

2.5.1.11. Maintain the appropriate security clearance for access to classified information and the base network. Personnel who refuse to complete a SF-86 via eAPP without sufficient justification will be disconnected from the network once their security clearance has been out of scope for six-months. The 374 AW/IP will notify individuals and the unit commander seven days prior to having network access disconnected to give the individual one last opportunity to comply.

2.5.1.12. Personnel contacted to complete a SF-86 via eAPP will be given two opportunities to submit and provide the required information of the initiated record. Subsequent requests will be made via memorandum by the USM and/or 374 AW/IP to: third request to the squadron commander, fourth request approved to the group commander, and the fifth/final request to the Wing Deputy Commander. Persistent refusal to submit security clearance background information are grounds to revoke a clearance IAW DoD 5200.02_DAFMAN 16-1405 and report the individual to the DCSA AVS for further action.

2.5.1.13. Personnel who have not had their clearance verified will not be granted access to classified areas, information, or to perform duties regardless of rank or position. If

personnel who have not had their clearance verified persist to gain access or force access to open storage areas or classified information, Security Forces will respond and take control of the individual(s). The Air Force Office of Special Investigations (AFOSI) will also be contacted to interview prohibited personnel about their intentions to access classified information. 374 AW/IP will review the incident to determine if a permanent security incident will be reported to the DCSA AVS in DISS.

2.5.1.14. All unit personnel must be aware of their responsibilities when handling, controlling, or possessing classified information/materials. Personnel requesting access must have their security clearance verified prior to granting access IAW DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 2. Entry Authority List (EAL) or DISS Visit Authorization Request (VAR) may be used to verify clearances. The 374 AW/IP staff or unit security managers may verify security clearances in DISS verbally over the phone when EALs or VRs are not immediately available as long as this is the exception and not the norm.

2.5.2. Reporting Security Incidents. Immediately report situations where sensitive information is found improperly safeguarded or appears to have been improperly accessed. The USM is the primary contact for collateral classified security incidents. The USM will notify 374 AW/IP within 24-hours as well as coordinate notification to the appropriate authority, depending on the category and type of information involved. If the USM is not available, report incidents as noted below:

2.5.2.1. If classified information is found improperly stored, accessed or marked, immediately secure it and report the incident to your USM, commander, supervisor or 374 AW/IP. If the incident involves a network system or includes network components the Wing Cybersecurity Office (WCO) must also be notified.

2.5.2.2. If the USM is not available when the initial notification is completed, ensure they are notified as soon as possible afterwards.

2.5.2.3. If the incident occurs after normal duty hours, secure the information in an approved storage container/area and report it the next duty day. The same requirements apply, regardless of the type of information, (i.e., hardcopy, electronic media, etc.).

2.5.2.4. If Personally Identifiable Information (PII), a form of CUI, is improperly secured, improperly accessed by unauthorized individuals, or improperly transmitted over Non-classified Internet Protocol Router Network (NIPRNET), i.e., is sent outside the AF Information Network to commercial addresses or other government agencies but not encrypted/digitally signed. The member must also contact the 374 AW Privacy Act Manager for specific actions to take. 374 AW/IP will also take required actions as the incident dictates.

2.5.2.5. All other types of CUI will be evaluated on a case-by-case basis with the originating agency to determine what, if any, administrative actions may be appropriate. If an unauthorized disclosure results in a public release of information, the 374 AW/IP office will be notified to ensure required notification to HQ PACAF/IP for further reporting to SAF/AAZ.

2.6. Security Container Custodians.

2.6.1. Custodians are responsible for ensuring all documentation and automated data

processing (ADP) media under their control, to include courtesy stored material, is properly marked, stored and safeguarded IAW Executive Order (EO) 13526, *Classified National Security Information*;

Information Security Oversight Office (ISOO) Directive Number 1, *Classified National Security Information, and* DoDM 5200.01V3_DAFMAN 16-1401V3.

2.6.2. Unit commanders will appoint in writing, Security Container Custodians (SCC); see **Attachment 5**. All personnel having access to the combination of the container, open storage area/vault and Secret Internet Protocol Router Network (SIPRNET) lockbox are not required to be listed on the letter. The signed letter will be forwarded to the 374 AW/IP for tracking and inspection purposes. At least one primary will be appointed to maintain oversight of each container or open storage area or vault. There is no limit to the maximum number of personnel assigned as security container custodians but should be kept to a minimum necessary to enhance safeguarding and accountability of classified information.

2.6.3. There are no specific rank requirements for SCC(s), but they must have a current security clearance eligibility at the same level or higher of the material appointed over and should have at least one-year retainability. The appointment letters will be sent to the 374 AW/IP staff who will in-turn provide training materials to all SCC(s) upon receipt.

2.6.4. Training. Security Container Custodians will complete the Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) Marking Classified Information Course (IF105.16)/Course Exam (IF105.06) and the Storage Containers and Facilities Course (PY105.16)/Course Exam (PY105.06) within 60 days of being appointed as a custodian. USMs will annotate the custodian's training date on their copy of SCC appointment letter and maintain a copy of the training documentation (certificates). The DCSA CDSE training courses are located at: **https://www.cdse.edu/index.html** .

2.6.5. Technical Assistance. Security Container Custodians will work any needed technical assistance through their USM. Direct contact with the 374 AW/IP by the custodian is not authorized; this insures USM is aware of any issues with security containers under their cognizance.

2.6.6. Container Maintenance/Administration. Custodians will comply with DoDM 5200.01V3_DAFMAN 16-1404V3 when accomplishing container maintenance, to include use of the OP Form 89 and other required security forms.

2.6.7. Maintain and update a record of authorized individuals having access to the container combination IAW DoDM 5200.01V3_DAFMAN 16-1404V3. A copy will be maintained in the security container and in the USM continuity book.

2.6.8. Ensure all documents/items stored in the container are properly marked, IAW DoDM 5200.01V3_AFMAN 16-1404V2, and this instruction.

2.6.9. Ensure when the required annual classified "clean-out" day is conducted as noted in **paragraph 9.8.5** to verify only information needed for specific mission requirements is maintained.

2.6.10. Commanders must provide an updated appointment letter to 374 AW/IP, within 30 days of any change (addition/deletion) in personnel with knowledge of, or access to, their respective GSA security container combination.

2.7. Information Protection Training.

2.7.1. Initial and Annual Information Security Training: The 374 AW/IP Training Program covers all training requirements outlined in DoD and AF instructions and consists of Initial/Indoctrination Training, and Annual Refresher Training. Select personnel will require additional focused training based on job responsibilities (e.g., security managers, couriers, security container custodians, etc.).

2.7.2. Initial Training: Newly assigned personnel must receive initial security training by respective unit security managers per paragraph 10.2 of this instruction.

2.7.3. Annual Refresher Training. All personnel must receive annual security training by following guidance in paragraph 10.2.2 of this instruction. Unit security managers will track completion of training to show type of training, rank, name of individual trained, and date training was completed.

2.8. Commander Inspection Program (CCIP).

2.8.1. Under the CCIP, an IP inspection will be conducted on an annual basis by the 374 AW/IP for units that process or store classified material on Yokota AB. At a minimum, CCIP consists of requirements as outlined in the unit security managers continuity book, prescribed forms, requirements for open storage areas, custodian appointments and training, the training program, security clearance requirements, reproduction and destruction procedures, marking of equipment used to manage classified equipment including AIS.

2.8.2. USMs will be responsible for conducting semi-annual IP self-assessments. An IP self-assessment checklist as well as the IP MICT checklists are located on the 374 AW/IP SharePoint website.

2.8.3. The 374 AW/IP uses the annual IP inspection as the primary source for collecting required data used to complete the annual Information Security Oversight Office (ISSO) report mandated by the National Security Council and IAW DoDM 5200.01V1_AFMAN 16-1404V1, Enclosure 2.

Chapter 3
INFORMATION SECURITY (INFOSEC) PROGRAM

3.1. Policy And Program Management. This chapter establishes guidance for protection of classified information and outlines the responsibilities of Yokota AB personnel in relation to complying with the INFOSEC program as outlined in DoD and AFI governing directives. The Yokota AB INFOSEC program is a part of the overall SECENT program and applies to all assigned units, to include tenant units, as required under base support agreements between the tenant unit and 374 AW.

3.1.1. Policy. These policies/philosophies apply to protecting classified information and controlled unclassified information under the purview of relevant statutes, regulations, and directives.

3.1.2. Program Management. Unit INFOSEC programs are an integral part of the overall unit SECENT program and will be managed IAW Executive Order (EO) 13526, DoD/AF implementing guidelines, supplements and this instruction. Commanders will consider corrective actions and sanctions as outlined in the basic guidance if individuals are found to have willfully or negligently violated rules of conduct in regard to controlling access, protecting, handling, safeguarding or transmitting material addressed under IP guidance IAW DoDM 5200.01_DAFMAN 16-1404, Volumes 1 through 3.

3.1.2.1. The CIP provides oversight for the INFOSEC program through 374 AW/IP, which is the primary focal point for INFOSEC issues at Yokota AB. The Wing INFOSEC Specialist:

3.1.2.1.1. Acts as the primary INFOSEC coordinator for the CIP by coordinating/managing INFOSEC program reviews/CCIPs events.

3.1.2.1.2. Coordinates, monitors and validates unit responses in regard to deficiencies noted due to classified security incidents, CCIPs, or HHQ inspections.

3.1.2.1.3. Acts as the primary INFOSEC training coordinator and develops and distributes local course curriculum, as needed.

3.1.2.2. The USMs act as unit INFOSEC representatives and then CIP provides oversight to ensure they provide INFOSEC programs management on behalf of their unit commanders.

3.2. INFOSEC-Related Programs. The INFOSEC Specialist assigned to 374 AW/IP is the primary focal point for INFOSEC matters at Yokota AB. Additional duties and responsibilities for units are provided in upcoming chapters 7 through 11 which includes handling/storing sensitive information (classified or unclassified); marking, transmitting, safeguarding, training of sensitive information and the classified security incident program. These items are addressed in separate chapters to help clarify specific responsibilities but are all integral parts of the INFOSEC and overall Yokota AB SECENT program.

Chapter 4
PERSONNEL SECURITY (PERSEC)

4.1. Policy and Program Management. This chapter establishes guidance for completion of Personnel Security Investigations (PSIs) and processing personnel to meet clearance eligibility needs. The Yokota AB PERSEC program applies to all assigned members, including active duty/guard/reserve military personnel, civilian employees and contractors.

4.1.1. Criteria for Application of Security Standards. The criteria for determining eligibility for access to classified are found in DoDM 5200.02_DAFMAN 16-1405, as supplemented by Security Executive Agent Directives (SEAD) 4, *National Security Adjudicative Guidelines*, SEAD 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position* and SEAD 8, *Criteria for Temporary Eligibility* (formerly interim). All commanders must apply these standards when granting access to classified, to include ensuring reporting occurs as outlined in SEAD 3.

4.1.2. Program Management. The Yokota AB PERSEC program is managed by 374 AW/IP Wing PERSEC Specialist for the CIP, IAW DoDM 5200.02_DAFMAN 16-1405, *Department of the Air Force Personnel Security Program (PSP);* DoDM 5200.01_AFMAN 16-1404, Volumes 1-3, *Information Security Program*; supplementing DoD and AF guidance and this instruction.

4.2. Duties and Responsibilities. The CIP implements and provides oversight of the PERSEC program on behalf of the 374 AW/CC through the 374 AW/IP PERSEC Specialist. Tenant units must comply with Yokota AB PERSEC program requirements to receive support from 374 AW/IP.

4.2.1. Commander and Staff Agency Chief Responsibilities. Referred to as commanders for the remainder of this chapter, Commanders and Staff Agency Chiefs implement and provide oversight of the PERSEC program for their units through their appointed USM. This includes completion of required self-assessments (SAs), preparation for SAs and CE monitoring/reporting requirements associated with DoDM 5200.02_DAFMAN 16-1405, Section 2.13.i., and SEAD 3.

4.2.2. Servicing Security Activity. The 374 AW/IP PERSEC Specialist acts as the Servicing Security Activity for Yokota AB PERSEC program on behalf of the CIP.

4.2.3. Authorized Requestor. The 374 AW/IP is the only authorized requester for Yokota AB PSI Tier 3 and Tier 5 actions unless authorization granted for Group and Squadron users. Specific actions and responsibility are outlined in DoDM 5200.02_DAFMAN 16-1405, Section 5.2.

4.2.3.1. If a tenant unit is supported by the 374 AW/IP, the fact they will comply with local requirements will be outlined in the Base Support Agreement.

4.2.3.2. If a tenant unit performs their own PERSEC functions, no PSI support is provided by the 374 AW/IP. This will be confirmed in an IP support exemption memorandum. This does not preclude providing technical assistance on a short-term basis, mission permitting, e.g., fingerprint service support, clearance eligibility verification, etc., whenever situation arises where the tenant temporarily loses this capability.

4.2.3.3. The 374 AW/IP and 374 FSS Civilian Personnel Flight (CPF) are designated as

the submitting agencies for Tier 1, 2 and 4 (non-sensitive) PSI cases per 374 AW/CC Tier Policy Letter.

4.2.3.4. The CPF will submit PSI and complete Tier 1 requirements for GS employees, non-appropriated employees, 374 FSS contracted employees. Also, will complete FSS childcare requirements and monitor Government of Japan Master Labor Contract (MLC)/Indirect Hire Agreement (IHA) T1 equivalent and childcare requirements.

4.2.3.5. The 374 AW/IP will submit PSI and complete Tier 1 requirements for non-374 FSS assigned contractors, volunteers (military & civilian) and specialized military positions (i.e. SAR, SAPR, Chaplain Corps employees, Limited Chapel volunteers and Military Treatment Facility members (requiring contact with children).

4.2.4. Unit Security Managers. The USM is the focal point for management of the unit PERSEC programs.

4.2.4.1. Unit members will route any questions for 374 AW/IP through their USM first, they will NOT contact the 374 AW/IP directly.

4.2.4.2. Members must complete required training outlined in DoDM 5200.02_AFMAN 16-1404 and this instruction before being indoctrinated for access in the database.

4.2.4.3. If derogatory information brings a member’s trustworthiness, loyalty, or honesty into question, commanders will make required Continuous Evaluation (CE) notifications and evaluate whether access should be suspended IAW DoDM 5200.02_DAFMAN 16-1405, Section 9.2.d.(1) and the adjudicative guidelines outlined in SEAD 4. The Wing PERSEC Specialist assists USMs and commanders with review of the adjudicative guidelines when derogatory information is received on members and determining if reporting is required IAW SEAD 3.

4.2.4.4. Access to special material will be based on the specific rules for the specific program.

4.3. Management of the Database of Record. The Defense Investigative Service System (DISS) or successor system National Background Investigation Services (NBIS) is the "database of record".

4.3.1. Notifications. Commanders will ensure unit procedures require the USM be notified of any of the following:

4.3.1.1. In/out-processing of unit members or position changes which place assigned military or civilian members in a new UMD position. This ensures the database of record properly reflects status of all assigned unit personnel.

4.3.1.2. Discovery of potential derogatory information concerning assigned unit members. This ensures adjudicative guidelines are reviewed and CE reports are accomplished.

4.3.1.3. Decisions on whether access to classified and/or computer systems will continue if a CE or other report of potential derogatory information is generated. This ensures any access is considered against the applicable adjudicative guideline.

4.3.1.4. Failure to notify the USM of these items may result in unauthorized access to sensitive information, which may cause a classified security incident and, IAW SEAD 3, a CE report on the individual who failed to make the notification.

4.3.2. Unit Management. The USMs are the unit's sole focal point for managing database of record. They must maintain their unit’s data IAW DoDM 5200.02_DAFMAN 16-1405, supplemental guidance and in this instruction.

4.3.2.1. The USM is responsible for adherence to all requirements of DoDM 5200.02_DAFMAN 16-1405, as supplemented and this instruction. This includes, but is not limited to, the following:

4.3.2.1.1. In/out-processing unit personnel into/out of the DISS or successor system NBIS.

4.3.2.1.2. Using the investigation closed date in database of record to determine when unit members are submitted for periodic review (PR) investigations.

4.3.2.1.2.1. Note: If enrolled for Deferred Investigation, the PR due date is based on the Deferred enrollment date. If enrolled for “Other”, regardless of the enrollment date, the PR due date is based on the last Investigation Closed Date.

4.3.2.1.3. Updating, monitoring and acting on notifications received in the database of record for assigned personnel (e.g., CE notifications, in/out-processing, completing SF 312 if needed, etc.).

4.3.2.1.4. Recording and removing applicable accesses IAW with database of record requirements, e.g., using the grant access link, including any applicable special access programs.

4.3.2.1.5. Annotating completion of the SF 312, *Classified Information Nondisclosure Agreement* (NDA) in the database of record using the grant access link and mailing completed NDAs on a weekly or monthly schedule to: AFPC/DP1ORM, 550 C Street West, JBSA-Randolph TX 78150.

4.3.2.1.6. Tracking visit authorization access request notifications in the database of record. This may include sending, receiving or rejecting the VAR, as required.

4.3.2.1.7. The unit commander is responsible for ensuring the USM monitors and updates DISS or successor system NBIS for SEAD 3 Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position.

4.3.2.1.8. The USM will not upload CE incidents; the Wing PERSEC Specialist will oversee upload of these reports.

4.3.2.2. The USM will protect all information associated with the database of record as PII (mark CUI) and report improper release or access as a PII breach to Wing Privacy Manager and 374 AW/IP.

4.3.2.3. The USM will be responsible to ensure units sponsoring classified mass briefing events use procedures found at **paragraph 4.8** below to allow entry to the briefing.

4.3.3. Controlling Database of Record Information. The database of record is a real-time system which is continuously updated. Printing hard copy products for use in validating access levels defeats the purpose of the system’s real-time function and is prohibited, IAW database rules.

4.3.3.1. Hard copy products will NOT be printed to be used by personnel/agencies to verify

clearance data. Security clearance can only be validated by the USM via the system of record.

4.3.3.2. The USM will ensure personnel not performing USM duties who require access to DISS or successor system NBIS are processed as follows:

4.3.3.3. The commander submits a request letter to 374 AW/IP stating personnel listed require "read only access." Access will be granted using Security Officer Visit Admin access in DISS or successor system NBIS.

4.3.3.4. The USM will complete the DD Form 2962, *Personnel Security System Access Request*, and validate appointed individuals have completed required training identified on the USM training tracker for Security Officer Visit Admin access.

4.3.3.5. The USM will maintain a copy of the appointment letter and training certificates in the USM continuity binder. The 374 AW/IP will maintain a copy of the appointment letter in the applicable PERSEC sharepoint folder.

4.4. Processing PSIs. The USM will use the National Background Investigation Services (NBIS) eApplication (eApp) to submit, track and process security clearances initial or PRs. This requires completion of actions in a timely manner to prevent negative impact on daily mission, TDYs, deployments, etc. The guidance in DoDM 5200.02_DAFMAN 16-1405 requires personnel to have at least 1-year retainability in order to submit a package in eApp, no exceptions.

4.4.1. Submission of PSIs. The USM submits Tier 3 and 5 personnel for initial or periodic review PSIs based on assigned UMD SAR codes.

4.4.1.1. Investigative request will not be submitted for eligibility higher than what has been designated for the position or required for the duty to be performed.

4.4.1.2. In the case of civilian employees hired where a UMD SAR code does not yet exist for the job, the PD on file with the Civilian Personnel Flight (CPF) may be used to determine authorized access levels until the UMD is updated.

4.4.1.3. If there is a conflict between the UMD and PD, the UMD takes precedence. If the position is term hire the PD is used to grant access.

4.4.2. Individual Responsibilities. Each member must complete paperwork associated with a PSI eApp within established timelines, failure to complete reinvestigation requirements could result in a CE incident for Personal Conduct “failure without reasonable cause to complete security forms.

4.4.3. Initial Tier 3 and Tier 5 Civilian PSIs. PSIs for civilian employees requiring a Tier 3 or Tier 5 PSI are reviewed and submitted by the 374 AW/IP in collaboration with CPF.

4.4.3.1. The CPF will validate the member does not have an existing, valid PSI in the database of record before submitting for an initial PSI.

4.4.3.2. Access to SECRET material requires a SAR code 7 on the UMD and a current or submitted Tier-3 PSI.

4.4.3.2.1. Prior service members hired for a SAR code 7 UMD position with an in-scope (less than 10 years old) Tier-3 or Tier-3R or Tier-5 do not require a new PSI

unless there was a break in service of over 24 months.

4.4.3.2.2. Members selected for a SAR code 7 UMD position not meeting one of the above requirements must be submitted for a Tier- 3 PSI **before** being eligible for temporary SECRET access.

4.4.3.3. Access to TOP SECRET requires a SAR code 5 on the UMD and the member must be submitted for a Tier-5 PSI.

4.4.3.3.1. Prior servicemembers filling a SAR 5 code UMD position with an in-scope (less than 5 years) SSBI, Tier-5 or Tier-5R do not require a new PSI unless there was a break in service of 24 months or more.

4.4.4. Documentation of PSI Forms. The USM is responsible to ensure required forms and documentation are properly accomplished for submitted PSI requests. This includes:

4.4.4.1. Ensuring all forms (e.g., NDA, AF Form 2587, *Termination of Security Access*, etc.) are accomplished and maintained as required.

4.4.4.2. Use procedures from AFMANs 16-1404 and 16-1405 for completing and maintaining forms.

4.4.5. Unacceptable or Discontinued Cases. The 374 AW/IP will contact applicable USM immediately for further instructions if a case is returned by Office of Personnel Management (OPM) as unacceptable or discontinued.

4.4.6. Contact with Adjudicators. The 374 AW/IP staff is sole focal point for contacting DCSA Adjudication and Vetting Services (DCSA AVS) priority tracking program or making inquiries to OPM concerning Tier 3 and 5 cases. The USM will never contact these agencies unless directed to by 374 AW/IP in response to requests for information by the agencies.

4.4.7. Timelines for eApp submission. Failure to comply with local timelines will result in the eApp account being terminated. The 374 AW/IP may modify these timelines, if verifiable justification is provided by the USM on why an extension is required. The local procedures are:

4.4.7.1. The USM makes the request to 374 AW/IP for first time establishment of the account.

4.4.7.2. If the initial account terminates, the unit commander must request reopening.

4.4.7.3. The second time an account terminates, the 374 AW/IP PERSEC Specialist will notify the unit commander, through the USM, to consider CE actions under the Adjudicative Guideline of "Personal Conduct" for failing to complete/provide security background information.

4.4.7.3.1. Once the commander completes the CE evaluation, a third account will be established.

4.4.7.4. If there is a third time an account terminates, the 374 AW/IP CIP will notify the 374 AW/CD of a negative trend for CE consideration under the noted Adjudicative Guidelines and a failure to comply/obey with lawful order.

4.4.7.5. The noted eApp procedures apply ONLY to accounts which are generated under oversight of the SMO YM0RFC1G for the 374 AW/IP.

4.4.7.6. The USM will use the following rules for submitting PSIs:

4.4.7.6.1. All eApp requests must be submitted to 374 AW/IP PERSEC Specialist.

4.4.7.6.2. The 374 AW/IP PERSEC Specialist attempts to create the account on day received or as mission allows in timely fashion.

4.4.7.6.3. Once created, member has 5 calendar days to enter account, or it automatically terminates (per NBIS eApp).

4.4.7.6.4. Once member enters account there are 10 days to complete upload and review by USM (per NBIS eApp).

4.4.7.6.5. Once uploaded the 374 AW/IP PERSEC Specialist will conduct final review and will submit to National Background Investigations Bureau (NBIB) or defer the investigation, as appropriate, within 2 weeks and notify member and USM of submission date.

4.4.8. Interim Eligibility for Temporary Access. The following procedures to grant interim eligibility for temporary access to classified are IAW DoDM 5200.02_DAFMAN 16-1405, Section 7.16. The USM will ensure:

4.4.8.1. All interim eligibility requests are coordinated through the 374 AW/IP PERSEC Specialist prior to initiating a commander's risk assessment.

4.4.8.1.1. The owning unit commander completes a risk assessment based on available information using the Adjudicative Guidelines, SEAD 8 and DAFMAN 16-1405 to DoDM 5200.02.

4.4.8.2. A commander's risk assessment is completed and includes a review of the member's completed SF 86, along with the AF Form 2583, until a final adjudication is received. Submit package to 374 AW/IP.

4.4.8.3. Access will NOT be granted prior to completion of these mandatory actions under no circumstance.

4.4.8.4. Interim Eligibility access is documented using the completed SF 86, AF Form 2583, SF 312 and adding the member to any applicable unit classified access lists.

4.4.8.5. Provide the member a copy of the completed SF 86 and AF Form 2583, regardless of approval or disapproval. Also, a copy of the signed commander’s letter, as the required written notification of the decision per DoDM 5200.02_DAFMAN 16-1405, Section 7.16, paragraph 7.

4.4.8.6. Interim Eligibility for SECRET access requires verification of acceptable proof of citizenship (USM), a completed SF 86 with favorable review, a completed local base records check, initiation of the required investigation AND completion of a favorable FBI fingerprint check. ALL these actions MUST be completed BEFORE the commander can grant approval of interim eligibility.

4.4.8.7. Interim Eligibility for TOP SECRET access requires completion of all requirements cited for SECRET. Also requires completion of a favorable National Agency Check (NAC). ALL these actions MUST be completed BEFORE the commander can grant approval of interim eligibility.

4.4.9. Suitability, Adjudication and HSPD-12 PSIs. The 374 AW/CC designates 374 FSS CPF as the lead agency responsible to process Tiers 1, 2 and 4 suitability/adjudication determinations IAW DAFGM 2023-36-03 and 5 CFR Part 731. The 374 AW/IP can only provide advice and guidance for making T1 suitability and fitness determinations. They are prohibited from making any fitness and suitability decisions IAW DoDM 5200.02_DAFMAN 16-1405 and DAFGM 2023-36-03.

4.4.10. Fingerprint Services. The background/fingerprint checks for childcare positions as well as T1, T3, T5 background investigations can be scheduled via 374 AW/IP Fingerprint Services online appointment site at https://374awip.setmore.com.

4.4.10.1. NAF applicants, employees and Youth Program volunteers are directed to contact NAF HR Office for scheduling of Fingerprint Services.

4.4.10.2. DoDEA applicants and employees are directed to contact DoDEA Pacific Personnel Security Specialist at 225-5779 for Fingerprint Service appointments.

4.4.10. Child and Youth Program (CYP) PSIs. These investigations are related to suitability and adjudication and conducted by NAF Human Resource Office IAW guidance found in DAFI 34-144, *Child and Youth Programs*, for employees and/or volunteers working with/around children under NAF Child and Youth Program on Yokota AB.

4.4.11. Suitability Determinations. If OPM or the FBI fingerprint check is returned with derogatory information on an applicant a suitability determination is required.

4.4.11.1. A suitability determination is also required if OPM does not return a favorable adjudication on an investigation.

4.4.11.2. The 374 FSS/FSC will coordinate with units on actions required for suitability cases using their standard operating procedures.

4.5. Continuous Evaluation and Reporting Requirement. All personnel must continuously monitor themselves, others, and report any potentially derogatory information to the USM, supervisor or commander as soon as possible after the event. Additionally:

4.5.1. Commander Responsibilities. Unit commanders must establish procedures to ensure required notifications are made in the appropriate database as outlined in DoDM 5200.02_DAFMAN 16-1405, Section 11; Security Executive Agent Directive (SEAD) 3 & 4; and this instruction. This includes documenting travel outside the US, disclosure of foreign contacts and CE up/down-channel notifications. If potentially derogatory information is reported the commander will:

4.5.1.1. Use the SEAD 3 and SEAD 4 adjudicative guidelines, in collaboration with 374 AW/IP PERSEC Specialist to determine if a CE report is initiated. This determination must be completed within 72 hours of receipt of unfavorable information (i.e., 3 duty days) if foreign intelligence entity is involved.

4.5.1.2. Determine whether access is formally suspended or not upon initial determination. Once access is formally suspended in the database of record, it may only be reinstated by DCSA AVS.

4.5.1.2.1. Commanders may locally or formally suspend access at a later date if additional derogatory information is uncovered.

4.5.1.2.2. Access may be locally suspended by the commander IAW DoDM 5200_DAFMAN 16-1405, Appendix 7A, Paragraph 7A.2.a.(1).

4.5.1.3. Notify the 374 AW/IP PERSEC Specialist to ensure all required CE notifications are accomplished. Also consider coordinating with the 374 AW Judge Advocate (JA) prior to taking formal suspension actions to ensure due process for the member is protected.

4.5.1.3.1. If the member is Sensitive Compartmented Information (SCI) indoctrinated or has access to a Special Access Program (SAP), also notify these program managers (i.e. Wing SSO or 5AF GSSO) of the decision.

4.5.1.4. Include a requirement for other unit agencies, e.g., First Sergeant, supervisors, etc., to notify the USM in the unit's SECENT OI, if applicable. This will ensure any potentially derogatory information can be reviewed against Adjudicative Guidelines to determine if CE reporting is required. Also ensure:

4.5.1.4.1. The OI provides USM access, as needed, to personnel records needed to determine eligibility and reliability; it is acceptable for the USM to go through a focal point (e.g., first sergeant) for access to this type of information.

4.5.1.4.2. The OI clarifies reporting of this information within specified CE program timelines is mandatory and failure to report within timelines may generate a CE report on the individual who failed to report.

4.5.1.4.3. The OI clarifies the USM will contact 374 AW/IP staff for technical assistance if unsure on actions to take or unclear on whether SEAD 3 and SEAD 4 criteria apply.

4.5.1.5. Ensure procedures are in place to notify the USM for CE reporting purposes when a member is suspected of abuse or misuse of a government issued credit card or spending accounts IAW DoDM 5200.01_DAFMAN 16-1405, Section 11. This should be included in the unit SECENT OI.

4.5.1.6. Ensure procedures are in place to deny access and initiate a CE report for any individual who refuses to sign an NDA. This should be included in the unit SECENT OI.

4.5.2. USM Responsibilities. The USM will:

4.5.2.1. Review derogatory CE information received against SEAD 3 and SEAD 4 adjudicative guidelines, and recommend appropriate actions to the commander and assist with up channeling notifications through the 374 AW/IP to DCSA AVS.

4.5.2.2. Ensure an AF Form 2587 is completed anytime a CE action results in suspension of access to classified information.

4.5.2.3. Notify the 374 AW/IP PERSEC Specialist when an individual with an open CE report is projected for permanent change of assignment/station, deployment or TDY.

4.5.2.3.1. Ensure 374 AW/IP receives a memorandum from the commander at least 10 days prior to the member's departure.

4.5.2.3.2. Ensure a copy of orders is received as soon available so 374 AW/IP can forward the CE to the gaining base to allow the gaining unit commander to review the CE contents.

4.5.3. Counterintelligence (CI) Reporting. Security professionals at Yokota AB will share potentially derogatory information discovered with each other and with the lead Yokota AB CI agency (AFOSI Detachment 621). The CI agency will share information with the 374 AW/IP PERSEC Specialist, if sharing the information does not violate the integrity of an on-going investigation.

4.5.3.1. The 374 AW/IP staff will notify the CI agency when potentially derogatory information of a criminal nature is reported on members through the adjudicative process.

4.5.3.2. The 374 AW/IP will notify the CI agency if a security incident report indicates an unauthorized disclosure occurred due to a member improperly releasing or mishandling classified or sensitive information. Security incident reports will be made available to the CI agency, upon request.

4.5.3.3. If the CI agency takes action on CE notifications provided by the 374 AW/IP office they should provide a case number, which is required by the DCSA AVS.

4.5.3.4. The CI agency will ensure commanders are aware of the need to consider adjudicative guidelines for actions which result in investigation. This may be accomplished by including the CE requirement on the checklist used to brief commanders.

4.6. Granting Access.

4.6.1. Identifying Access Levels for Positions. Commanders determine the level of access necessary for each military and civilian position based on the mission needs. The commander reflects these decisions on the UMD by ensuring position numbers carry the appropriate SAR.

4.6.1.1. Civilian positions also have a position sensitivity identified on their PD which must match the SAR code on the UMD. The USM must work closely with supervisors when position descriptions are created to ensure the proper PS code is reflected on the PD. If there is conflict between the UMD and PD, the UMD takes precedence until the conflict is resolved.

4.6.1.2. Access may never exceed the SAR code for the position. For example, if a unit member has TOP SECRET eligibility but is assigned to a UMD position allowing only SECRET-level access—they may only be granted SECRET access. Additionally, reinvestigations for the individual will be based on the current UMD SAR code of SECRET—not the previous eligibility of TOP SECRET.

4.7. Yokota AB AFB Visit Request/Servicing Plan. When distinguished visitors, inspection teams or other groups are scheduled to visit Yokota AB, and will need access to classified information, use the following procedures to ensure they can gain authorization for access.

4.7.1. Inspection Teams. The USM responsible for the organization being inspected will receive the team visit authorization request in DISS or successor system NBIS for the duration of the visit and will validate the DISS or successor system NBIS access matches the access listed on the Entry Authorization List (EAL).

4.7.1.1. If the inspection is wing-wide the primary host USM will receive the DISS or successor system NBIS visit authorization request and conduct the validation. Also, they will ensure a copy of VAR is passed to 374 AW/IP.

4.7.1.2. If the inspection is unit-specific (e.g., one specific squadron or group being

inspected), the USM for the inspected agency will receive the DISS or successor system NBIS visit authorization request and will conduct the validation.

4.7.2. Special Visits. If a special speaker or event requires mass briefings of classified, the USM for the unit sponsoring the event is responsible for ensuring personnel attending send a visit authorization request for the event. The sponsoring USM will validate clearance access for all attendees.

4.7.3. Validation Procedures. Find and accept the VAR and verify the individual is indoctrinated and meets minimum requirements outlined on the inspection EAL or the event EAL. If issues are noted; DO NOT accept the visit and contact the event sponsor. Examples of issues include:

4.7.3.1. The individual does not have the required investigation for the briefing level.

4.7.3.2. The individual is NOT indoctrinated at the proper level for briefing (e.g., indoctrinated to SECRET, but briefing is at TS level).

4.7.3.3. A completed SF 312 is not showing in the system for the member.

4.7.3.4. The briefing contains special access information (e.g., NATO, etc.) but the member is not indoctrinated for the needed access.

4.7.4. Mass Briefings of Classified for Local Units. It is acceptable to use the above procedures to generate an access list for allowing entry to local classified briefings.

4.8. Limited Access Authorization (LAA). A process that enables a non-U.S. citizen to have limited access to classified information, but it is not a national security eligibility.

4.8.1. An LAA may be granted, in rare circumstances, when:

a. A cleared or clearable U.S. citizen is not readily available or does not possess the skills or expertise required.

b. The non-U.S. citizen possesses unique skills or expertise needed to support a specific U.S. Government requirement involving access to classified information.

4.8.2. When a unit/organization wants to request a LAA for a non-U.S. citizen, the USM will notify 374 AW/IP so processing will occur IAW DoDM 5200.02_DAFMAN 16-1405.

4.8.3. Processing time for LAA nominations varies on a case-by-case basis but averages between 8-12 months.

4.9. Unofficial Foreign Travel. IAW DoDM 5200.02_DAFMAN 16-1405, Section 11.6 (e), all unofficial foreign travel will be reported in DISS. The following requirements must be completed prior to commanders' approval (can be delegated to unit security manager) of member's foreign travel.

4.9.1. Member should notify their USM of their planned unofficial foreign travel 30 days prior to the start of travel (does not apply to trips inside Japan; Okinawa, Osaka, Sapporo, etc).

4.9.2. Member must submit to USM a complete itinerary, dates of travel, mode of transportation, passport data (number, approval & expiration date, passport type), names and association of any foreign traveling companions, planned contacts with foreign governments, or citizens during the trip and reason for such contact, and emergency point of contact information.

4.9.3. Member must receive a foreign travel briefing from the Air Force Office of Special Investigations (AFOSI). This can be accomplished by going to AFOSI Foreign Travel Brief website at: https://usaf.dps.mil/teams/foreigntravel/SitePages/ForeignTravelBriefs.aspx#/.

4.9.4. IAW INDOPACOM instruction 5050-08, all active duty servicemembers are required to register on TT/IATP website at: https://iatp.pacom.mil.

4.9.4.1. Visit Department of State website and review information pages on applicable destination country.

4.9.4.2. Visit DoD Foreign Clearance Guide to see if any additional requirements are mandated for the specific destination country. Note: You will be required to create an APACS account before access to the DoD FCG is granted. The website is https://apacs.milcloud.mil/fcg/loginForm.cfm.

4.9.5. Recommend registration with the DoS Smart Traveler Enrollment Program (STEP) at:

https://step.state.gov/.

4.9.6. Member will notify their USM of completion of requirements.

4.9.7. USM will have member review and sign an Unofficial Foreign Travel Acknowledgement Sheet, thus approving the member's foreign travel.

4.9.8. USM will enter trip data into the member's DISS record.

4.9.9. Upon completion of trip, member will be required within 5 days to complete a post-travel brief via the aforementioned AFOSI website. Member will forward a copy of the completion e-mail to USM.

Chapter 5
INDUSTRIAL SECURITY (INDUSEC) PROGRAM

5.1. Policy and Program Management. This chapter establishes guidance for implementing the National Industrial Security Program and outlines the responsibilities of Yokota AB personnel in relation to integrating contractors into the SECENT program.

5.1.1. Policy. It is AF policy to identify what access industry (i.e. contractors) will have to information or sensitive resources (regardless of classification, sensitivity, physical form, media or characteristics) which must be protected against compromise and/or loss while entrusted to industry in the performance of classified contracts.

5.1.1.1. The primary focus of INDUSEC is to review contracts working with classified (cleared), but technical assistance for contracts not dealing with classified (uncleared) may be provided, as manning allows. The Yokota AB INDUSEC program applies to all assigned units, to include tenant units, as required under base support agreements between the tenant unit and 374 AW.

5.1.1.2. Prior to allowing access to contractors, a valid need-to-know (NTK) requirement must be established. A valid DD Form 254 or visit authorization request, or other local document, is used to verify contractors are authorized access and meet all local access requirements IAW DoDM 5220.22,Volume 2_AFMAN 16-1406, Volume 2, Sections 4 & 5.

5.1.2. Program Management. This program is managed IAW DoDM 5220.22V2_AFMAN 16-1406V2, as supplemented, and this instruction.

5.1.3. Scope. The security polices, requirements and procedures identified in this chapter apply to all AF personnel and any on-base DoD contractors performing services at Yokota AB under the terms of properly executed contract and DD Form 254 and associated security attachments or similar document as determined appropriate by the installation commander. Access to classified/sensitive material will be denied if it is not clear whether the required contractor has the required investigation; if it is unclear whether the required DD Form 254 has been completed and copy provided to 374 AW/IP or host unit per DoDM 5220.22V2_AFMAN 16-1406V2.

5.2. Duties And Responsibilities.

5.2.1. The 374th Airlift Wing Commander. The 374 AW/CC responsibilities are outlined in DoDM 5220.22V2_AFMAN 16-1406V2, Section 2.8.e.

5.2.1.1. The CIP is delegated all duties and responsibilities for the INDUSEC program on behalf of the Wing Commander.

5.2.2. CIP Duties. The CIP implements and manages the Yokota AB INDUSEC program on behalf of the 374 AW/CC. In addition to the above delegated duties, the CIP is responsible for items outlined in DoDM 5220.22V2_AFMAN 16-1406V2, Section 2, paragraph 2.8.f.

5.2.3. Yokota AB Contracting Officers. The contracting officer responsibilities are outlined in DoDM 5220.22V2_AFMAN 16-1406V2, Section 2, paragraph 2.8.g. and include the following:

5.2.3.1. Negotiate contractual agreements, blanket purchase agreement, modifications, changes, revisions with all contractors assigned to Yokota AB.

5.2.3.2. Notify 374 AW/IP within 30 days anytime an initial review of an agency's proposed statement of work (SOW) or performance work statement (PWS) indicates a job will require a contractor to have access to classified material. Depending on classification level, collaboration with Wing Special Security Officer (SSO) or 5 AF Government Special Access Program Security Officer (GSSO) may be required. This must be accomplished prior to the award of a contract.

5.2.3.3. Provide 374 AW/IP with a current copy of the SOW or PWS.

5.2.3.4. Inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the classified contract.

5.2.3.5. Serve as the Approving Official for the DD Form 254 and ensure it is prepared and distributed IAW DoDM 5220.22V2_AFMAN 16-1406V2.

5.2.4. Commander Responsibility. Commanders will ensure assigned personnel comply with this instruction and the DoD/AF basic directives when allowing contractors access to classified. Management and oversight of the unit INDUSEC program is accomplished through their appointed USMs and unit contracting representatives.

5.2.5. Program/Project Manager Responsibility. Program/Project Managers are key to identification of specific types of information required by the contractor and provide security classification guidance by developing the DD Form 254**.** Program/Project Managers will:

5.2.5.1. Prepare the DD Form 254 ensuring security requirements specific to the contract are included. Ensure coordination with other stakeholders is conducted as required.

5.2.5.2. Review security violation reports, and other products received from DCSA via 374 AW/IP indicating classified information related to an Air Force contract is at risk of or has been the subject of loss, compromise, or suspected compromise. Prepare a response to DCSA on behalf of the information owner (i.e., OCA) documenting the conduct of a classification review and a decision regarding whether a damage assessment was required IAW DoDM 5220.22V2_AFMAN 16-1406V2. Disseminate the response to DCSA via 374 AW/IP who will coordinate through MAJCOM (HQ PACAF) information protection channels.

5.2.5.3. Report changes through information protection channels to DCSA that could affect the FCL of a cleared contractor, including but not limited to indicators of FOCI; federal law enforcement investigations of the company or its key management; debarment or exclusion of a cleared contractor; a company's request to terminate the FCL; etc.

5.2.6. USM Duties. The USMs are responsible for complying with the DoDM 5220.22V2_AFMAN 16-1406V2 and this instruction. If new classified contracts are being planned, the USM will ensure the 374 AW/IP is immediately notified. They will also:

5.2.6.1. Verify all contractors are indoctrinated in the database of record for the level of access to classified stated on the DD Form 254 and are debriefed, as required.

5.2.6.2. In collaboration with 374 AW/IP assist in ensuring applicable requirements of DoDM 5220.22V2_AFMAN 16-1406V2 and this instruction are adhered too, and applicable contractor employees are compliant.

5.2.6.3. Ensure a Visitor Group Security Agreement (VGSA) or local document in lieu of, is established with each Visitor Group (VG) performing duties for the unit to cover local security requirements. 374 AW/IP will provide documentation to USM. This documentation will:

5.2.6.3.1. Clarify, define, and expand security and training requirements from SOW and DD Form 254 to ensure all local requirements are included.

5.2.6.3.2. Participation in annual unit self-assessments, CCIP events and/or inspections.

5.2.6.4. Maintain all VG documentation in the USM continuity book.

5.2.6.4.1. If the unit has no industrial contractors on active classified contracts, the USM will place a Memorandum for Record (MFR) in the Tab of the continuity book stating the "Unit has no active classified industrial contracts."

5.3. Cleared Contractor Access. Prior to allowing access to Yokota AB classified, the USM will take the following actions for cleared contractors to ensure access is authorized:

5.3.1. Database of Record Management. The USM will advise the 374 AW/IP of visit authorization request changes (i.e., new or terminated employees) and update DISS. The USM will use the following procedures for updating DISS:

5.3.1.1. Verify the contractor has the correct investigation for the level of access specified in the DD Form 254 and has completed any required training before in-processing to servicing or allowing access to classified material.

5.3.1.2. Input cleared contractors to "owning" relationship status in DISS for the duration of the visit authorization request or DD-254. This ensures the unit are notified on any changes to status. Ensure 374 AW/IP is notified accordingly.

5.3.1.3. When employees are terminated the USM will accomplish the following:

5.3.1.3.1. Remove employee "owning" relationship from DISS.

5.3.1.3.2. Notify 374 AW/IP of the change.

5.3.1.3.3. Notify personnel where the contractor had access of the change of status and ensure security container custodians conduct an inventory of classified material.

5.3.1.3.4. Accomplish any other needed actions, e.g., change combinations to containers, update SF 700, etc.

5.3.2. Employee Status Changes. The USM will notify the Contracting Officer to ensure accomplishment of the following actions when an employee's status changes:

5.3.2.1. The contractor company's FSO provides updates to the visit authorization request any time employee's status changes occur.

5.3.2.2. The FSO security representative completes any needed administrative actions if access is terminated, e.g., AF Form 2587, etc.). If the security representative is not

available (e.g., single-person VG) the USM performs this function. In either case, the USM will maintain a copy of the documentation.

5.4. Reporting Requirements. The 374 AW/IP via USM will ensure the VGSA or local documentation covers the following reporting requirements.

5.4.1. Security Incidents. Ensure procedures outlined in **chapter 11** of this instruction are used if a security incident with classified information is suspected concerning contractors on Yokota AB.

5.4.2. Cleared Contractor Responsibilities. Cleared contractor working at Yokota AB will notify the servicing USM of any classified security incidents and take actions IAW with this instruction.

5.4.3. Reporting Derogatory or CE Information. The FSO will ensure 374 AW/IP or applicable USM is notified of any incidents or information which is not local, but involves an employee authorized access on the visit authorization request.

5.4.4. HHQ Reporting. The 374 AW/IP will up-channel local cleared-Contractor incidents to HHQ IAW DoDM 5220.22V2_AFMAN 16-1406V2.

5.4.5. Procedures for Suspicious Contacts. Report any cleared contractor involved in suspicious contacts/events, such as possible espionage, suspected sabotage, acts of terrorism, or subversive activities, IAW DoDM 5220.32, Volume 1, Section 8.2.

5.5. Contractor Release of Information. Contractor's requests for public release of information will be IAW DoDM 5220.32, Volume 1, Section 6.5. Contractors who receive requests for release of public information will follow the requirements outlined on block 12 of the DD Form 254/local requirements.

5.6. Unclassified (Uncleared) Contracts. These are contracts which do not require contractors to access classified information but still require access to the installation, the Air Force Network (AFNET), or special areas. The 374 AW/IP is not manned to provide support for these contracts. However, technical support may be provided, as manpower allows, at the request of 374th Contracting Squadron (374 CONS).

5.6.1. Review of Uncleared Contracts. If an INDUSEC review of an uncleared contract is accomplished, it will be based off the requirements in the PWS/SOW provided by 374 CONS.

5.6.1.1. The security review will focus on items such as need for access to CUI material, defining CUI protective requirements, outlining OPSEC requirements and establishing minimum needed security training and/or education, etc.

5.6.2. Homeland Security Presidential Directive 12 (HSPD-12) Requirements. Any agency other than 374 CONS which solicits contracts at Yokota AB (e.g., Army Air Force Exchange Services (AAFES), Defense Commissary Agency (DECA), etc.) will notify the 374 FSS/FSC if the initial review of the contract appears to require the contractor/company to need access to the installation or CUI material. The agency soliciting the contract will ensure the PWS addresses the fact the contractor must meet the background check requirements outlined in HSPD-12.

5.6.3. Trustworthiness Determinations. If an uncleared contractor requires a Tier 1, 2 or 4 PSI, the USM will process the PSI using procedures noted in **chapter 13** of this instruction.

Chapter 6
CYBER SECURITY

6.1. General Information. Information, regardless of its format, will be protected IAW guidelines established in DoDI 5200.48_DAFI 16-1403, DoDM 5200.01_AFMAN 16-1404, Volumes 2 and 3, as applicable.

6.2 . Document Imaging Devices Used with Sensitive Data. Refer to DoDM 5200.01_AFMAN 16-1404, Volume 2, Enclosure 3, Section 18 and Volume 3, Enclosure 7, for specifics on equipment such as fax machines, copiers, scanners, automated information systems (AIS), etc., used with classified. Comply with 374 CS guidance and DoDI 5200.48_DAFI 16-1403 for CUI.

6.2.1. Reproduction. Printers, copiers, scanners, and fax machines retain data. Equipment account holders must ensure these devices are properly sanitized when taken out of service in accordance with DoDM 5200.01_AFMAN 16-1404, Volumes 2.

6.2.1.1. Prior to releasing printers, copiers, scanners, and fax machines to any other agency, the unit is responsible for sanitizing the equipment IAW cybersecurity guidelines. Unit Cybersecurity Representatives (CRs) may contact the Wing Cybersecurity Office (WCO) for guidance.

6.2.2. Printers/Copiers/Scanners and Fax Machines used to Process Classified Data. Copy machines/scanners approved for classified use must reside in a Classified Processing Area (CPA) and have a hard drive sanitization kit installed that purges all memory/hard drives after each use.

6.2.2.1. Additionally, a copier must have an approval letter which:

6.2.2.1.1. States the copier INFOSEC checklist (see **Attachment 6**), was used by the USM to determine the copier meets minimum standards.

6.2.2.1.2. Includes clearing instructions, (e.g., minimum number of blanks needed to purge latent images or any other requirements).

6.2.2.1.3. Is signed by the unit commander.

6.2.2.2. Copiers/scanners approved for classified use must also be clearly identified with a sign stating, "authorized for classified use”.

6.2.2.3. If both classified and unclassified copy machines/scanners are collocated in an area, each device will be clearly identified as either approved or not approved for classified use. Unclassified copiers in a classified processing area will ALWAYS be labeled as "NOT AUTHORIZED FOR CLASSIFIED USE."

6.2.2.4. If the copier/scanner is networked, it must be marked and protected IAW AIS marking, and protection standards discussed in paragraph 6.3 below

6.2.4. Multi-Function Device (MFD), e.g. Digital Senders, are only authorized for use with CUI on NIPRNET if they have CAC authentication and are properly configured IAW the guidance in Security Technical Installation Guides (STIG) and AFMAN 17-1301.

6.2.4.1. If MFDs retain data, the hard drive must be properly sanitized when retired IAW AFMAN 17-1301.

6.2.4.2. MFDs must have an appropriate classification label (such as SF 710, *Unclassified* (label), SF 702, *Controlled Unclassified Information* (label) or SF 707, *Secret* (label)) and DD Form 2056, *Do Not Discuss Classified Information* (label).

6.2.5. Collaborative Computing. DAFMAN 17-1301, para. 4.12. This term refers to applications and technology (e.g., whiteboarding, group conferencing) that allow two or more individuals to share information in real-time in an inter- or intra-enterprise environment. (CNSSI No. 4009). The use of cameras or microphones in areas where classified information is processed (electronically or hardcopy) is not authorized unless the following considerations are addressed.

6.2.5.1. The computer used is a SIPRNET computer and all personnel in the vicinity of the session are cleared at the appropriate level and have a valid need-to-know.

6.2.5.2. Use of collaborative systems on NIPRNET computers is authorized for text transmission in classified areas, provided the sender does not transmit classified information over the uncleared computer and the following considerations are addressed.

6.2.5.2.1. Peripherals must be acquired through AF Information Technology Commodity Council enterprise buying programs, such as GSA Advantage.

6.2.5.2.2. Embedded collaboration equipment must be physically disabled and/or removed. Peripherals are not allowed to be cross shared between networks or classification levels.

6.2.5.2.3. Peripherals must be wired. No wireless peripherals are allowed**.**

6.2.5.2.4. Headsets and microphones. Must be an external device and not embedded in the computer. Must have Push to Talk (PTT) or Positive Disconnection Device (PDD) capabilities. PTT and PDD capabilities must operate through physical means and not software. Must not contain any noise-cancelling functionality.

6.2.5.2.5. Webcams must be an external device and not embedded in the computer. Must have PDD capabilities. Must only be used in private offices or conference rooms and not face any open doors and/or windows.

6.3. Marking AIS Equipment/Media. The minimum markings required for AIS equipment and media used for classified are outlined in DoDM 5200.01V2_AFMAN 16-1404V2 and will be applied as explained in chapter 8 below. Use rules from DoDI 5200.48_DAFI 16-1403 for CUI.

6.4. Cellphones and Electronic Devices in Classified Processing Areas (CPAs). Unauthorized devices pose a particular threat to sensitive information due their small size and the inherent risk they present to national security information. Any unauthorized government or personal electronic device found in a CPA is subject to the posted installation search and seizure guidelines and failure to surrender the device may result in apprehension by Security Forces and confiscation of the device. Disposition of the device is discussed under classified security incident for CPAs below.

6.4.1. A CPA is defined as an area which contains computer or electronic devices that process classified information, where classified hardcopy material is worked on or where classified conversations routinely occur. Some examples include the use of secure communication devices (e.g. VoSIP), a work center where classified hardcopy is reviewed, conference rooms where classified meetings are held and/or SIPRNET computers used.

6.4.1.1. Failure to comply with CPA requirements will result in security incident. Items located in the CPA must be specifically authorized on the TEMPEST certification package.

6.4.2. Electronic Items in CPAs. Unless specifically authorized on the TEMPEST package, it is prohibited to introduce any electronic devices which operate on radio frequency (RF) and infrared (IR) bands or which have photographic or audio recording capabilities (e.g., cell phones, wireless keyboard/mouse, etc.) into CPAs. The authorized user must properly sanitize and secure the area of unauthorized devices before classified information is processed/discussed (e.g., SIPR tactical local area network encryptor (TACLANE) keyed with Crypto Ignition Key (CIK))

6.4.2.1. Personal electronic or data devices are never authorized in CPAs.

6.4.2.2. Ensure personnel are reminded prior to CPA entry or CPA activation to check for cellphones, as they are a specific threat and commonly used by all personnel.

6.4.2.3. Hand-held radio transceivers, used with intra-base radios and land-mobile radios, deserve special consideration because of their unique operational applications. A person may carry these devices into a CPA only if they are on the approved.

6.4.2.4. Government issued Electronic Flight Bag (EFB) program devices (i.e., iPads) must be removed from CPAs unless they are specifically approved on the area's TEMPEST package. In unit specific open storage areas, they may “transit” a hallway in the “off” position. They are also authorized for transit through flight line areas and for use on aircraft so long as configured IAW the Authority to Operate. See **Attachment 7** for further guidance on EFB program.

6.4.2.5. SIPRNET users must acknowledge understanding of responsibilities and security requirements when they sign the Rules of Behavior and Acceptable Use (RBAU) Agreement, AF 4394 (Air Force user Agreement Statement – Notice and Consent Provision) provided by 374 CS. Also, complete Cyber Awareness training and submit DD Form 2875 (System Authorization Access) to 374 CS/WCO.

6.4.2.6. Users must understand that a TACLANE and a CIK in the same location makes them classified. They are required to maintain positive control (i.e. personal observation and physical control) of the TACLANE and CIK. The failure to maintain positive control (personal observation and control) will result in a security incident.

6.5. Documenting System Access. Use the DD Form 2875 to document system access requests. These forms are processed to grant users specific permission levels on a specified IT system. Specifically:

6.5.1. Processing NIPRNET DD Form 2875s. The unit CR will maintain these forms. Follow the form’s instructions and the following steps. 6.5.1.1. USM Actions. The USM will verify investigation meets the minimum of a Tier-1 or higher investigation. Also, completion of Cyber Awareness and Initial Orientation training per paragraph 10.2.1.3 of this instruction.

6.5.1.1. Cybersecurity Representative Actions. The CR will ensure the DD Form 2875, and the user agreement form is properly filed.

6.5.2. Processing SIPRNET DD Form 2875s. The unit CRs and 374 CS/Communication Focal Point (CFP) will maintain copies of these forms.

6.5.2.1. If SIPRNET access is being granted, the USM will annotate block 21 with following statement, **"The USM signature above also verifies initial security orientation, derivative classification training and NATO brief were completed IAW DoDM 5200.02V3_DAFMAN 16-1404V3."**

6.5.2.2. If the USM fails to validate required training prior to SIPRNET access, or improperly validates an investigation for a member, it may result in a security incident and/or negative derogatory actions on the USM.

6.6. Negligent Discharge of Classified Information (NDCI) Handling Procedures. An NDCI occurs when classified data enters an information system for which it is not accredited to process.

6.6.1. The specific details of any NDCI are classified until the affected systems are cleared which requires secure communications be used for all notifications.

6.6.2. All computers suspected of being involved in a NDCI will be treated as classified as soon as the incident is declared.

6.6.3. Computers will not undergo sanitization by 374 CS/WCO until 374 AW/IP has concurred all investigative procedures have been completed.

6.6.4. The Communications Focal Point (CFP) is the lead agency for NDCIs that occur on NIPRNET and SIPRNET. The CFP will notify the 374 AW/IP when they are made aware of an NDCI as soon as possible.

6.6.5. Procedures. Due to the dynamic environment associated with cyber-risks, the AF NDCI process is very fluid and requires the CFP to assess each situation, as it occurs, against the current 624th Operations Center tasking orders (TASKORDs) to determine local responses. As a minimum, ensure the following actions are accomplished when a potential NDCI is reported:

6.6.5.1. Personnel will immediately notify CFP, USM, or CR of any potential NDCI.

6.6.5.2. The USM or CR will immediately notify their commander and then notify the CFP to state there is potential for a NDCI. NOTE: No details or discussions of the incident will be discussed over the phone unless using secure phones. The discussion over unsecure phone lines can and will lead to a security incident.

6.6.5.3. The USM will also notify 374 AW/IP NLT 24 hours.

6.6.5.4. The 374 AW/IP will always verify that the 374 CS/CFP is aware of any NDCI reported to them by USMs or other personnel.

6.6.5.5. Air Force Mission Assurance Center (AMAC) directs all sanitization actions and is responsible to notify any other bases affected.

6.7. Non-Traditional Work Environments. Use of any secure device in an environment typically considered not the normal work environment (i.e., office, secure area, etc.) constitutes use in a non-traditional work environment and requires consideration of requirements outlined in DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 7, Section 7 or Enclosure 2, Section 12 (when applicable). Note the approval of such environment is based on justification on a case-by-case situation. The situations include use of documents or a non-mobile secure device at a home location (e.g., VIPER phone, SIPRNET or classified documents used in a commander's home), use of a secure portable electronic device (PED) at a home or undesignated location (e.g.,

SecureView). In all of these cases, a risk assessment by 374 AW/IP and 374 CS/WCO is required. In the case of home or PED use, HQ PACAF/IP must approve the use after the risk assessment is completed via the residential storage process.

6.7.1. Use of Non-mobile Classified Devices/Material in a Residential Environment. A site survey meeting all requirements will be accomplished, IAW DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 7, before requesting PACAF/IP approval for residential use as discussed in DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 2, Section 12. Contact 374 AW/IP to request the required residential storage site survey. 374 AW/IP will coordinate with 374 CS/WCO to address any potential TEMPEST concerns.

6.7.1.1. Installed devices require a TEMPEST survey and will not be moved or added without prior coordination through 374 AW/IP and 374 CS/WCO.

6.7.2. Use of Secure Portable Electronic Devices (PEDs). Consider the following:

6.7.2.1. Regardless of whether the PED will be used in a residential or undesignated setting, a site survey will be accomplished, and HQ PACAF/IP approval is required.

6.7.2.2. If the secure PED will be used in a residential setting, a site survey will be conducted, and a designated CPA established. The secure PED may only be used at the residence in the designated CPA.

6.7.2.3. If the secure PED is intended for undesignated location use, a site survey of the device will be conducted to establish needed countermeasures.

6.7.3. Establishment of Temporary TEMPEST Sites. Upon notification of planned event (i.e. exercises), immediately contact 374 CS/WCO to commencing planning of temporary TEMPEST Site. In the event of emergency operations, contact the 374 CS/WCO for immediate assistance.

6.7.3.1. Contingency TEMPEST CPAs are used only in tactical or deployed environments and will comply with AFSSI 7702, Attachment 2.

6.7.3.2. Users will comply with the contingency TEMPEST rules, where possible, even during actual contingency environment. Users will notify WCO for instances not met.

6.7.3.3. Physical security rules for protection of classified still apply during contingency operations.

6.7.4. Storage Requirements. Storage requirements vary with device types. Follow all requirements as outlined in the site survey.

6.7.5. The crypto ignition key (CIK) for a SIPRNET terminal, along with the TACLAN or an access code for PEDs are considered classified when in proximity of the device. If they are written down and/or left unattended within physical proximity of a secure PED a security incident will be declared.

6.7.5.1. Follow rules outlined in the site survey for storage of CIKs.

6.7.6. Reporting Loss of Device/Compromise. Take the following actions regarding suspected loss or compromise.

6.7.6.1. If a secure PED is lost, stolen or tampered with, immediately notify the 374 CS/WCO and USM.

6.7.6.2. If the access code or CIK are lost, immediately notify the 374 CS/WCO.

6.7.6.3. If a keyed device (VIPER, PED or SIPRNET) are discovered unattended while keyed, immediately report the incident to the USM.

6.8. Cyber Security Incident. A cyber security incident is any violation regarding network policy on NIPRNET or SIPRNET. These types of events may include items such as external media violations, unapproved software, NDCI violations, and improper use of network access.

6.8.1. For all Data Loss Prevention (DLP) violations or incidents which do not involve classified but may involve is not limited to, plugging in unapproved external hard drives, thumb drives, mobile devices, dongles, or adapters, etc. The 374 CS/WCO will follow the most relevant TASKORDs that outlines the remediation procedures. The violating individual will be required to re-accomplish their cybersecurity awareness training before access is renewed to the network.

6.9. Network Access Suspension. This applies when a member's access is suspended.

6.9.1. Classified Systems. If the member's eligibility for access to classified is suspended, denied, or revoked the individual's USM will ensure the commander, and 374 CS/CFP are informed and classified system access is immediately suspended.

6.9.2. Unclassified Systems. When access to classified is suspended or revoked, the USM and 374 AW/IP will coordinate with their commander to determine if access to NIPRNET will be maintained.

6.9.2.1. If the commander determines NIPRNET access is suspended, the USM and/or 374 AW/IP will contact 374 CS/CFP for access removal processing.

6.9.2.2. If commander wishes to reinstate NIPRNET access before classified access is reinstated, they must request NIPRNET reinstatement from the Information System Security Officer (ISSO). The ISSO would process accordingly.

6.10. Portable Wearable Fitness Devices (PWFD) and Electronic Medical Devices (EMD). In Open Storage Areas (OSAs) and Classified Processing Areas (CPAs), all PWFD and EMD requests must be reviewed by 374 AW/IP and 374 CS/WCO. In Sensitive Compartmented Information Facilities (SCIF) and/or Special Access Program Facilities (SAPF), approval authority lies with Wing Special Security Officer (SSO) and applicable Government Special Access Program Security Officer (GSSO) respectively. All PWFD and EMD requests must be processed IAW DAFGM2024-16-01.

6.10.1. Members requesting/needing approval for a PWFD or EMD will contact their USM to obtain either the DAF Form 110, *DAF EMD Request Form & Approval Card*, or DAF Form 111, *DAF PWFD Request Form & Approval Card*.

6.10.2. The USM will provide appropriate DAF Form 110 or 111 along with a request memorandum. The requesting member will complete the form, update memorandum, sign and submit to their USM who will review and submit to 374 AW/IP.

6.10.3. 374 AW/IP will process request and will coordinate with WCO for TEMPEST approval IAW DAFGM2024-16-01.

6.10.4. Upon approval 374 AW/IP will provide guidance to USM along with approval memorandum and signed DAF 110/111 form. USM will present to requestor and obtain their acknowledgement.

6.10.5. Requester must maintain a copy of approved request on their person when in approved secure areas and should reapply for approval 30-days before their current approval expires (annually or when device is updated or replaced).

6.10.6. An unapproved PWFD/EMD entering an OSA, CPA, SCIF, or SAPF will be processed for a classified security incident and may result in further administrative actions.

Chapter 7
CLASSIFYING, MARKING AND DECLASSIFYING INFORMATION

7.1. Classification. There are two types of classification: Original and Derivative.

7.1.1. Original Classification. Only an Original Classification Authority (OCA) with delegated authority over the material can make the decision to classify information. This authority cannot be delegated. Yokota AB does not have any OCAs assigned. The Commander, Pacific Air Forces is the only authorized OCA for Pacific Air Forces. Since Yokota AB does not have an OCA assigned, a local Security Clearance Guide (SCG) cannot be produced, YAB must use the PACAF SCG. In the event Yokota AB personnel determine a category is not covered by the PACAF/SCG, a request to have the information included as a category will be made to HQ PACAF/IP through the 374 AW/IP.

7.1.2. Derivative Classification. Derivative application of classification markings is a responsibility of all assigned personnel who incorporate, paraphrase, restate, or generate in new form any information that is already classified or those who apply markings according to OCA guidance. The following requirements must be considered when making derivative classification decisions:

7.1.2.1. Generating Derivatively Classified Documents. Derivative classifiers must be specifically trained and receive refresher annually IAW current DoD directives.

7.1.2.2. Specific training requirements are outlined in **chapter 10**, **paragraph 10.3**, of this instruction. Derivative classification is extremely important to ensure classified information is provided the proper level of protection.

7.2.1.2. Derivative classifiers are responsible to ensure the proper markings are applied to all portions of the document and must understand failure to properly mark a derivative document may constitute a security incident.

7.2.1.3. The unit commander will appoint derivative classifiers in writing and USMs will maintain a compiled listing of unit members identified and trained to act as derivative classifiers, with a copy provided to 374 AW/IP.

7.2.1.4. The USM will verify members gaining access to SIPRNET have completed required training and annotate the DD Form 2875, block 21, with the statement, shown in previous **paragraph 6.5.2.1**.

7.3. Marking Classified Information. Derivative classifiers are required to verify documents they use comply with guidelines for marking found in the basic instructions.

7.3.1. Marking Requirements. Specific marking requirements can be found in DoDM 5200.01V2_AFMAN 16-1404V2.

7.3.2. Marking Classified E-mails. Information sent/received via approved secure communications systems must be properly marked. The receiver will notify the sender of

improper marking issues upon receipt. If the sender refuses to correct improper markings, it may be considered a security incident on the sender.

7.3.3. Printing Classified E-mails. All printed e-mail documents must be marked IAW DoDM 5200.01V2_AFMAN 16-1404V2 regardless of whether markings show appropriately when printed. It is the holder's responsibility to ensure classified under their control is properly

marked.

7.3.4. Special Control and Similar Notices. See DoDM 5200.01V2_AFMAN 16-1404V2 for instructions on special notices for restricted data, formerly restricted data, and other types of information.

7.3.5. Marking Special Types of Materials. When marking automated information systems, audiovisual media, hardware, products, etc., use the guidelines described in DoDM 5200.01V2_AFMAN 16-1404V2.

7.3.6. Marking Foreign Government Information in DoD Documents. Use the guidelines described in DoDM 5200.01V2_AFMAN 16-1404V2 to control and mark this information.

7.3.7. Marking Blank Pages in Multi-page Classified Documents. If a document contains blank pages, they must contain banner markings (i.e., top/bottom) using one of the marking conventions outlined in DoDM 5200.01V2_AFMAN 16-1404V2.

7.3.8. Mark binders similar to file folders, but with an additional marking on the spine of the binder. Use classified cover sheets in lieu of marking file folders; ensure a cover sheet is attached to both the front and back cover of the file folder.

7.3.9. All Media (i.e., diskettes, compact discs, and removable hard disk drives) used in an accredited classified automated information systems (AIS) must be marked with the highest classification stored on the media. Standard Forms 706, TOP SECRET (Label)/712, Classified SCI (Label) etc., are used for the purpose of marking media or other ADPE devices that retain classified information. Only devices that store classified information must be marked with a label (i.e. zero clients do not have a hard drive and once disconnected are zeroed). These devices do not retain classified information and do not have to be locked up once disconnected from the network.

7.3.10. The security container custodian(s) must track and document, during a consecutive 2-week period each year identified by 374 AW/IP, the number of new documents derived from classified material within their area of responsibility. The 374 AW/IP will collect the data and report to PACAF/IP.

7.4. Declassifying, Downgrading or Regrading Information. Use the guidelines in DoDM DoDM 5200.01V2_AFMAN 16-1404V2 to declassify, downgrade or upgrade classified information.

7.5. Classification Challenges. The holder of an improperly marked classified or unclassified document shall contact the document's originator to obtain correct markings. If personnel feel a document needs a higher or lower classification or should be declassified, it is the individual's responsibility to challenge the classification using procedures in DoDM 5200.01V2_AFMAN 16-1404V2.

7.5.1. Mismarked Information. If information is received without proper markings, always attempt to resolve the situation at the lowest level possible. First, contact the sender to verify the markings. If this does not work, ask your USM to contact the agency's USM. If this does not work, your USM should contact 374 AW/IP for additional assistance.

7.5.2. Handling/Storing Challenged Information. If there is doubt on the validity of classification authority or level for material, or it is not possible to verify what level information should be protected at, protect the information at the highest suspected level until

clarification is received.

7.6. Marking CUI. Follow the guidelines in DoDI 5200.48_DAFI 16-1403 and 374 AW/IP Controlled Unclassified Information (CUI) Marking Guide (posted on 374 AW/IP SharePoint website), when handling, processing, and marking controlled unclassified information (CUI) when it is NOT included in a classified document. Some specific considerations include:

7.6.1. General CUI Marking Requirements. All CUI documents will have "CUI" on the top and bottom of each page the document and the first page will have the "Dissemination Information" discussed below. It is the responsibility of the originator/writer of the document/e-mail to determine whether the information qualifies for CUI status and to ensure markings are applied as required IAW DoDI 5200.48_DAF 16-1403. Additionally:

7.6.1.1. Do not apply CUI markings to documents or e-mails unless a specific rule from the CUI Registry is applicable, applied and included in the Dissemination Information block. Improper use of CUI markings may result in administrative or other sanctions.

7.6.1.2. If one paragraph is marked parenthetically, all paragraphs must be marked parenthetically (i.e. portion marking). Use (U) for information which is not CUI in this case.

7.6.1.3. The CUI Designator Block will consist of the following:

7.6.1.3.1. Line 1: Controlled By: Service branch of the controlling agency and enter the office symbol of the agency controlling the information (for example, USAF // 374 AW/IP).

7.6.1.3.2. Line 2: CUI Category(ies): Obtain these by reviewing the CUI Registry and choosing those which apply—there may be more than one. For example, PII would be "PRVCY". The CUI Registry is found at **https://www.dodcui.mil/CUI-Categories-and-Abbreviations/**.

7.6.1.3.3. Line 3: Limited Dissemination Control: Commonly use "FEDCON" or other controls as applicable IAW DoDI 5200.48_DAFI 16-1403.

7.6.1.3.4. Line 4: POC: Include name, phone and/or email address of the individual to contact if questions are raised on the assigned category.

7.6.1.4. All e-mails sent over NIPRNET to outside the AF Network to commercial addresses or other government agencies containing any category of CUI must be digitally-signed and encrypted. Due to the underlying encryption native to the Outlook tool suite, there is no need to encrypt when sending messages to users on the AF Network domain.

7.6.2. Privacy Act Data/PII. Additional requirements over those in DoDI 5200.48_DAFI 16-1403, for this type of CUI are found in DoDM 5400.11, Volume 2 and AFI 33-332, *Air Force Privacy and Civil Liberties Program*. This includes:

7.6.2.1. Do not apply CUI PRVCY markings to documents or e-mails unless a specific rule from the CUI Registry is applicable, applied and included in the Dissemination Information block. Improper use of CUI markings may result in administrative or other Privacy Act notifications.

7.6.2.2. The writer must also identify which paragraphs contain the CUI information by placing (CUI) before the affected paragraph (i.e. portion markings).

7.6.2.3. If the information will be released outside DoD channels include the expanded statement from DoDM 5400.11, in addition to the CUI Designator block.

7.6.2.4. It is acceptable to use the expanded statement in an e-mail/hardcopy document, even if not going outside DoD channels provided the e-mail or document contains CUI information.

7.6.2.5. When e-mailing Privacy Act information over the AF Network, encryption/digital signature are not required but the sender must verify the receiver has an official need-to-know. If e-mailed outside the AFNET to other government agencies the sender must use DoDSAFE (**https://safe.apps.mil/**) to be able to encrypt the e-mail. Do Not send CUI outside AFNET in an unencrypted state.

7.6.2.6. Do not send Privacy Act information/PII to distribution lists or group e-mail addresses, unless each member is verified by the sender as having an official need for the information.

Chapter 8
TRANSMISSION/TRANSPORTATION OF SENSITIVE INFORMATION

8.1. General Policy. The DoD/AF general policy on transporting/transmitting classified or CUI is it should be sent electronically, Defense Courier Service (DCS), or through the U.S. Postal Service. When the use of these means is not feasible then couriering can be authorized on a case-by-case basis. Couriering is the exception and not met to be the norm.

8.1.1. Guidance. Personnel will use the procedures outlined in IAW DoDM 5200.01V3_ DAFMAN 16-1404V3, Enclosure 4, PACAF/IP guidance and this instruction when transporting or transmitting classified material. When transmitting CUI use the rules outlined in DoDI 5200.48_DAFI 16-1403, Section 4.1.e.(2).

8.1.2. Procedures. Unit Commanders must establish local procedures for sending and receiving classified information.

8.1.2.1. Use the unit's SECENT OI to address specific actions to take when receiving first class, certified or registered mail. These types of packages may contain classified and must be protected (at a minimum) as SECRET material until received by the designated office.

8.1.2.2. When transmitting/transporting specialized program information such as COMSEC, NATO, SAPs etc., collateral classified rules apply, in addition to any additional program requirements. If a conflict occurs, use the stricter of the two standards to ensure proper safeguarding.

8.2. Training. Commanders establish procedures and training in their unit's SECENT OI to ensure personnel tasked to send and/or receive sensitive information (classified or CUI) are properly identified, aware and trained, as needed. As a minimum, ensure the OI identifies:

8.2.1. Specific jobs requiring additional training, for example, secretaries, administrative assistants, receptionists and other personnel who perform administrative duties where U.S. mail is sent or received.

8.2.2. Procedures and training on actions to take when classified or CUI is received or sent. This will include procedures for receipt and protection of first class, registered or certified mail, which may contain classified or CUI information.

8.2.3. Training requirements for on-base couriering of classified is accomplished using a localized version of the 374 AW/IP Courier Training Brief and must be provided in-person by the USM. Training requirement for off-base couriers include the on-base requirements and the individual must also complete the CDSE on-line Transmission and Transportation for DoD Training found at **https://www.cdse.edu/Training/eLearning/IF107/**. All Yokota AB Courier training (on and off-base) must be completed annually and tracked by the USM.

8.2.4. Commander's Courier Briefing. This briefing will be documented using a briefing provided to USMs by 374 AW/IP. The member signs this briefing to acknowledge understanding of the training and the USM signs on behalf of unit commander to validate the training.

8.3. Standards. Each category of sensitive information (classified or CUI) has specific standards for transporting or transmitting. Consider the following when developing unit procedures for transmitting/transporting sensitive information:

8.3.1. Transporting/Transmitting of U.S. Collateral Classified. Off-base transport of classified is only authorized as a last resort or when other transport methods (i.e. electronic transmission, use of approved carrier service) are not viable. If required, transport will be accomplished using methods outlined in DoDM 5200.01V3_ DAFMAN 16-1404V3, Enclosure 4, PACAF/IP guidance and this instruction.

8.3.2. Transporting/Transmitting of Classified to Foreign Governments. Use only the methods outlined in DoDM 5200.01V3_ DAFMAN 16-1404V3, Enclosure 6, when considering how to transport/transmit classified material to foreign governments.

8.3.3. Transporting/Transmitting of CUI. Ensure the appropriate standard from DoDI 5200.48_DAFI 16-1403, Section 4.1.e.(2) **paragraph 7.6** (inclusive) of this instruction are applied before sending any unclassified sensitive information (i.e. CUI).

8.3.4. Improper Electronic Transmission of Information. If information is sent inappropriately over a computer, fax, electronic data device, or other electronic means follow the procedures outlined in chapter 6 of this instruction, depending on type and category of information.

8.4. Preparation For Shipment. When preparing classified material for physical shipment ensure the following:

8.4.1. Packaging. Comply with the requirements outlined in DoDM 5200.01V3_ DAFMAN 16-1404V3, Enclosure 4 when packaging classified material for shipment/transport.

8.4.1.1. In the case of bulky items or equipment, the outer cover may be a tarp or similar opaque covering to prevent the item from being viewed. The shell of an equipment item (i.e., aircraft part or laptop) may act as the "inner wrapper" provided it does not allow classified information or components to be viewed.

8.4.1.2. As a minimum, items not being mailed, but being shipped or moved as part of a daily operational missions (on or off-base), will utilize an inner and an outer cover.

8.4.1.3. Any material outside approved storage will be kept under personal observation and positive control by an authorized individual. Material will under no circumstances be left unattended while in transport. For example, member may not leave material "locked" in a vehicle, hotel safe or take material to a personal residence.

8.5. Courier Transport of Classified. Transport of classified occurs when an authorized and cleared individual moves classified from one location to another, either on or off an installation. On Yokota AB, both on and off installation transport require an individual to be appointed and trained as a courier. Courier will comply with the requirements outlined in DoDM 5200.01V3_ DAFMAN 16-1404V3, Enclosure 4, PACAF/IP guidance, and this instruction. Requirements do differ for on and off installation courier transportation and are determined on a case-by-case basis.

8.5.1. Administrative Requirements. Individuals must be cleared for access to the information transported, appointed by the owning commander/director/staff agency chief (delegated to USM for on-base) and have a commander briefing and courier training documented by the USM.

8.5.1.1. Commanders will identify all unit couriers (on or off-base) in writing. The appointment letter will be disseminated on a case-by-case basis. In rare instances where a standing appointment letter is created (approval must be coordinated with 374 AW/IP), the letter will be reviewed and updated on a monthly basis to mitigate the risk for potential

security incidents.

8.5.1.2. Off-base Couriers must also comply with additional requirements, to include:

8.5.1.2.1. An off-base commander appointment letter and briefing will be documented by the USM. The courier will keep a copy of the off-base courier appointment letter on them while performing off-base courier duties. The DD Form 2501, Courier Authorization Card will not be used for this.

8.5.1.3. Commanders must ensure briefcases and pouches used to transport classified (on or off-base) have an internal locking mechanism and that the exterior are properly marked with the unit's address, phone number, point-of-contact and that the case/pouch is serial numbered.

8.5.2. On-base Transport. This is the most common transport of classified and is defined within 374 AW/IP as a courier mission. It includes movement of classified between offices, buildings or between on-base geographic locations. The 374 AW/IP policy also requires specific administrative and training actions before unit members may move classified on-base. Specifically:

8.5.2.1. On-base Couriers will be appointed in writing by the unit commander, director/staff agency chief (can be delegated to USM for on-base courier missions only).

8.5.2.2. An annual courier briefing will be accomplished and documented using the template briefing provided by 374 AW/IP to USMs. This document must be signed by the member to acknowledge understanding of duties and training and signed by the USM to validate completion of the training.

8.5.2.3. In-person completion of the localized 374 AW/IP Basic Courier Training. Units may supplement (add to but not replace) this training with unit/section job-specific or specialized training (Maintenance, Command Post, Aircrews, etc.).

8.5.2.4. Use of POVs is authorized for transport of classified while acting as on-base courier, if GOVs are not available.

8.5.3. Off-base Transport. This occurs when a cleared and authorized member move classified from one installation/activity to another geographically separated installation or activity. Additionally:

8.5.3.1. It may be authorized by the owning commander only as a last resort, only when other authorized methods are not viable. For instance, hand carrying a classified document that could be sent as a secured transmission to the receiving location is not authorized. Additionally: 8.5.3.1.1. Comply with administrative requirements for on-base courier above (i.e., appointment, CC brief, training, etc.) Note: the courier training brief must be signed by unit commander (cannot be delegated to USM).

8.5.3.1.1. A Transportation Plan will be completed and must address deviations to travel plans and all other items outlined in the DoDM 5200.01V3_DAFMAN 16-1404V3, Appendix to Enclosure 4, Section 10.

8.5.3.1.2. The Unit Security Manager (Primary or Alternate) will inspect the classified for proper packaging and marking prior to packing.

8.5.3.1.3. A lockable briefcase/pouch will be used, if possible, but cannot serve as the

second layer of the double wrapping requirement.

8.5.3.1.4. The courier will receive and acknowledge the commander's off-base courier briefing.

8.5.3.1.5. The courier will use/comply with transportation log, two-person requirement or other requirements for off-base transport of SECRET, as noted within the DoDM 5200.01V3_DAFMAN 16-1404V3.

8.5.3.1.6. If flying the courier will use TSA pre-check (within U.S.).

8.5.3.2. If TOP SECRET information is being transported the owning commander will ensure compliance with 374 AW/IP specific requirements, such as:

8.5.3.2.1. Approval from 374 AW/CD if commercial travel is used to verify justification for this courier mission request.

8.5.3.2.2. Completion of required transportation plan.

8.5.3.2.3. Any other requirements outlined for off-base transport of TOP SECRET, as noted within the DoDM 5200.01V3_DAFMAN 16-1404V3.

8.5.4. Commercial Travel with Classified.

8.5.4.1. Failure to follow procedures in DoDM 5200.01V3_AFMAN 16-1404V3, applicable PACAF/IP guidance and this instruction may result in airport officials denying access to the mode of transportation or examining the classified package.

8.5.4.1.1. If airport security officials open the classified package report it as a security incident to the home station USM as soon as possible.

8.5.4.2. Comply with all 374 AW/IP specific transportation requirements (on case-by-case basis), e.g., waiver for TS to travel on commercial aircraft, use of TSA pre-check, two-person travel, etc.

Chapter 9
SAFEGUARDING SENSITIVE INFORMATION

9.1. General Policy. The AF policy for safeguarding is that each individual granted access to sensitive information (classified or CUI) is personally responsible to safeguard the material under their care from unauthorized access. This includes complying with special requirements associated with the material. Classified material will be stored only in approved storage containers or secure areas when not under the personal observation and control of an authorized person as outlined in DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 2.

9.2. Granting Access to Classified. Commanders will ensure the USM applies the standards found at Chapter 4 of this instruction to ensure compliance with DoDM 5200.01V3_DAFMAN 16-1404V3 and DoDM 5200.02_DAFMAN 16-1405.

9.2.1. Indoctrination to Database of Record. The USM is responsible for managing the in and out-processing of unit personnel into the database of record (i.e. DISS). Do not indoctrinate personnel for access or allow access to classified until all requirements from **Chapter 4** of this instruction are completed.

9.2.2. Verifying Clearances. Use only the database of record to verify individual clearances, regardless of whether an individual is permanent party, visitor, or an inspector. The database of record reflects changes in real-time which is why standing entry authorization lists are not used to verify clearances.

9.2.2.1. The USM may use procedures discussed at 4.3.3. and 4.8 of this instruction.to generate entry rosters.

9.3. Classified Aboard Aircraft. See DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 3, Section 6.a.(3), for specific rules concerning classified aboard aircraft.

9.3.1. At Yokota AB, Security Forces may conduct required checks **if** notified through prior coordination by the aircrew that classified material is present and the aircraft is sealed.

9.4. Closed Storage of Classified. Closed storage is defined as use of a GSA-approved security container for storage. Containers used to store classified must meet criteria outlined in DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 3. See paragraph 9.5 of this instruction for guidelines and procedures for requesting or using OSAs.

9.4.1. General Storage of Classified. The general requirements for storage of classified are discussed in DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 3.

9.4.2. Courtesy Storage. If classified belonging to one agency is stored in a classified security container controlled by another agency, a memorandum outlining the arrangement should be established. At a minimum it would need to address:

9.4.2.1. The routine protection, accessing, and emergency destruction of the classified.

9.4.2.2. The fact the agency providing storage is responsible only for physical security and access control of the material. All other administrative control/accountability requirements are the responsibility of the owning agency.

9.4.2.3. The measures established to prevent inadvertent or unauthorized access to the material; for example, sealing packages, separate locking drawers, etc.

9.4.3. "In Transit" Storage of Classified. This provision is provided for storage of classified received after duty hours, which cannot be stored in unit containers or for personnel who arrive unexpectedly with classified material and require storage.

9.4.3.1. The courier/custodian of the in transit classified will pre-coordinate a drop off with one of the agencies noted below to arrange temporary storage. Failure to pre-coordinate the drop off may result in refusal of the agency to accept the material. The courier/custodian will reclaim the material the next day or arrange for an authorized and cleared member to take control of the material.

9.4.3.2. Transient couriers requesting overnight temporary storage of classified material up to the SECRET Level will be directed to one of the following locations:

9.4.3.2.1. 374 OSS/IN, Bldg. 703, Duty Phone: 225-7711

9.4.3.2.2. 374 AW/CP, Bldg. 315, Duty Phone: 225-4343

9.4.3.2.3. 730 AMS/Special Handling, Bldg. 71, Duty Phone: 225-7070

9.4.3.3. 374 AW/IP can be contacted in emergency situations to determine a solution for safeguarding the classified material.

9.4.3.4. Unique Situations. In the event an aircraft carrying classified material lands unplanned at Yokota AB, and does not have a Protection-Level designation, the 374 AW/IP should be contacted if storage guidance is necessary. If the aircraft is transporting Sensitive Compartmented Information (SCI) or material that cannot be removed from the aircraft, the Defense Force Commander (DFC) will provide the level of security requested by the aircraft commander or senior Defense Courier Service (DCS) representative. Aircraft transporting SCI generally require Protection Level 2 guarding requirements unless the equipment can be zeroed -out. Commercial aircraft (not owned by the US Government) such as those in testing (e.g. KC-46 new tanker) with classified materials must still meet storage requirements while on Yokota Air Base.

9.4.4. Repairing Approved General Services Administration (GSA) security containers. The USM can work with 374 CES cleared technicians who may perform basic maintenance only without decertifying a container. Any modification or repair to a GSA-approved container (e.g., lock neutralization, welding, drilling, etc.) which does not comply with the Federal Standard results in the container being decertified. Immediate removal of classified contents will need to be executed by SCC and USM. 374 AW/IP notification is required.

9.4.4.1. If unauthorized work is suspected, immediately contact the 374 AW/IP to have the issue reviewed. 374 AW/IP will determine if the work requires recertification. If the container is decertified, it may not be used for storage of classified until recertified by a GSA-approved technician.

9.4.4.2. It is recommended to have a GSA-approved technician conduct a periodic maintenance inspection (PMI) on classified security containers once each 5 years. 374 AW/IP will coordinate via HQ PACAF/IP.

9.4.4.3. Use of a non-GSA locksmith to gain entry to locked out containers is authorized, however; the container must be decertified until reviewed by a GSA-certified technician.

9.4.4.4. Document all repairs, maintenance actions and combination changes on the OP

Form 89, *Maintenance Record for Security Containers/Vault Doors*, which replaced the AFTO Form 36, *Maintenance Record for Security Type Equipment*. Do not destroy old AFTO Form 36 documents, staple them to the new OP Form 89 as a historical record of maintenance (if applicable).

9.5. Open Storage (OS) of Classified. Classified material will not be stored outside an approved security container unless it is maintained in an authorized Open Storage Area (OSA). Only areas certified in writing by the 374 AW/CD or CIP are considered authorized. Due to the cost involved in establishing OSAs, they will not be approved for convenience. Commanders must notify the CIP, in writing, of any new OSA requirements and of any proposed changes to existing OSAs, prior to changes being made. The USM will ensure all approved OSAs are included on the unit consolidated container listing.

9.5.1. Initial Open Storage Area Surveys. The 374 AW/IP INFOSEC Specialist will conduct OSA surveys (along with applicable representatives from Yokota AB SECENT) and provide a written report listing required corrective actions/recommended fixes based on DoDM 5200.01V3_DAFMAN 16-1404V3, Appendix 1 to enclosure 3. All corrective actions must be addressed before the area will be certified by the 374 AW/CD or CIP for open storage.

9.5.1.1. Initial OSA surveys are conducted for facilities which do not currently exist, or which are being completely demolished and rebuilt.

9.5.1.2. There is no regulatory requirement for periodic OSA recertification surveys (i.e. every 3 to 5 years, etc). Instead, a recertification survey will only be conducted when a modification or change to OSA configuration is planned. 374 AW/IP will conduct a walk-thorough of approved OSAs during annual IP inspection. Substantial modification may include any changes which alter the layout of the interior impacting alarm coverage (e.g., moving furniture) or where the areas physical integrity is impacted (e.g., removal of doors, walls, windows, adding or removing vents, pipes, etc.). The USM must notify 374 AW/IP during the planning phase of any modifications being considered for an approved OSA. This is important to mitigate unnecessary cost and maintenance work.

9.5.1.3. The 374 AW/IP INFOSEC Specialist verifies corrective actions identified in the initial/recertification OSA survey are completed and notifies the CIP if the facility meets standards. The CIP will conduct final review of OSA Survey package and endorse the certification certificate. Facilities which do not meet standards will not be certified under no circumstance.

9.5.1.4. In some circumstances, temporary compensatory measures may be available until mandatory actions noted in the initial or certification surveys are complete. These types of measures are typically intended to be short-term (i.e., 30 days or less).

9.5.1.5. The USM will ensure specific written OS area entry and circulation controls are developed. These procedures may be included in an already existing unit OI.

9.5.2. Intrusion Detection Systems. Utilize the Protection Level 4 alarmed area rules found in Integrated Defense Plan for OSAs; with the following exceptions:

9.5.2.1. If alarms fail on a SECRET OSA, the USM or unit commander will contact the 374 AW/IP to determine if a cleared individual must be posted in the facility or if 4-hour checks of the facility by a cleared member (requires entry and walk-through) are authorized IAW DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 3, Section 3.

9.5.2.2. If alarms fail on a TOP SECRET OSA facility, the owner user must post a cleared individual in the facility. Checks of all vulnerable areas (e.g., doors, windows, vents, etc.) will be conducted at least once every two hours until alarms are restored.

9.5.3. Physical Security Checklist. The 374 AW/IP INFOSEC Specialist will conduct OSA surveys using standards derived from DoDM 5200.01V3_DAFMAN 16-1404V3, Appendix 1 to Enclosure 3 and other associated INFOSEC and PHYSEC regulations.

9.5.4. Certification/Recertification of OS Areas. The CIP certifies new OS areas and, if necessary, recertifies existing OS areas where substantial changes have occurred. Specific requirements are detailed below.

9.5.4.1. Commanders will not use areas for open storage of classified materials until certified by the CIP.

9.5.4.2. The CIP will certify OS areas once the 374 AW/IP OSA survey report indicates all corrective measures are completed and a visual certification has been completed by Wing INFOSEC Specialist.

9.5.4.3. Maintain initial, certification, supplemental and recertification surveys for OS areas at the facility, in the USM's program binder and in the 374 AW/IP sharepoint folder.

9.5.4.4. The unit commander, through the USM, will notify the 374 AW/IP of any "substantial" renovation, remodeling work proposed for approved unit OS areas. The notification must be given prior to start of modifications, preferably 30 days prior. This allows the 374 AW/IP sufficient time to determine what actions are required and which personnel are needed for the OSA survey. Include a detailed risk mitigation plan for protecting classified material/operations normally stored in the facility (if applicable).

9.6. Classified Processing Areas. An area defined as an area which contains computer or electronic devices that process classified information, where classified hardcopy material is worked on or where classified conversations routinely occur. It is not approved for open storage of classified information. It must be manned and meet safeguarding requirements during active processing of classified information.

9.6.1. CPA Physical Security Standards. CPAs on Yokota Air Base must pass information /physical security standards identified in 374 AW/IP CPA standards checklist; see **Attachment 8**.

9.7. Classified Discussions. In-office discussions of classified by personnel must ensure all participants in the conversation are properly cleared and have a valid need-to-know and that any classified conversation cannot be overheard by uncleared/unauthorized individuals.

9.7.1. No discussions that disclose classified or critical information will be held in general public locations to include: e.g., food court, exchange, commissary, post office, Kanto Lodge lobby, parking lots, etc.

9.8. Disposition and Destruction of Classified and CUI. Follow the guidelines in DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 3 when making decisions to retain and/or destroy sensitive material.

9.8.1. Central Destruction Facility. Yokota AB has an on-base incinerator which is available on a “by appointment” basis; phone: 225-7204. Also, an on-base shredder is available for large

amounts classified and CUI paper materials.

9.8.2. Information Technology Related Materials. Contact WCO for specific requirements to arrange for destruction of classified electronic media.

9.8.3. Destruction of CUI. Units must ensure comply with the standard outlined in DoDI 5200.48_DAFI 16-1403, paragraph 4.5(b), it states CUI, "…may be destroyed by means approved for destroying classified information or by any other means making it unreadable, indecipherable, and unrecoverable." This means any other methods which render the information unreadable, indecipherable, and irrecoverable would be authorized, however; use of a classified crosscut shredder is noted as meeting this standard.

9.8.4. Yokota AB has a standing 100% Shred Policy for all classified, CUI and handwritten documents (i.e. post-it, notepads, etc). Only food waste, wrappers, metal, glass, aluminum, and no-print items should be placed in trash receptacles. This helps mitigate the probability of classified, critical or controlled unclassified information being placed in the trash. Commanders and supervisors are expected to ensure approved shredders are readily available to unit personnel.

9.8.5. Annual Classified Clean-out Day. The classified clean-out date for Yokota AB is to be determined by 374 AW/IP (with 374 AW/CC concurrence) and completed on an annual basis each calendar year. The USM will ensure agencies are complying with this requirement during semi-annual IP self-assessments. The Classified Clean-out Day will be scheduled with an extended timeline to afford flexibility for Team Yokota units to complete within their high operations tempo. This is a mandatory annual event for participation by all 374 AW units, tenant units and encouraged participation by USFJ and 5 AF.

9.8.5.1. The 374 AW/IP will maintain records and review compliance with retention/destruction rules for classified during annual unit IP inspections.

9.9. Access Termination to Sensitive Information.

9.9.1. Access Termination to Classified. Refer to **chapter 6** of this instruction.

9.9.2. Access Termination to CUI. Individuals shall be debriefed with the following topics covered IAW DoDI 5200.48_DAFI 16-1403 and DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 2.

9.9.2.1. Remind individuals of their responsibility to continue to protect controlled unclassified information to which they had access.

9.9.2.2. Discuss procedures for reporting any unauthorized attempt to gain access to such information.

9.9.2.3. Remind individuals of the prohibition for retaining CUI when leaving the organization.

9.10. Alternative/Compensatory Control Measures. AF prohibits use of these measures.

9.11. Open Storage Area/Classified Processing Area Emergency Plans.

9.11.1. Emergency plans are required to be posted in all activity spaces that process or store classified information/material. Refer to DoDM 5200.01V3_DAFMAN 16-1404V3, appendix 2 for an emergency plan template that addresses the minimum plan requirements.

9.11.2. Ensure plan procedures also include a requirement to debrief and completion of a non-disclosure agreement if non-clear emergency personnel enter an OSA/CPA due to an emergency like fire/flooding/medical response and classified was present and exposed.

Chapter 10
SECURTIY EDUCATION AND TRAINING AWARENESS (SETA)

10.1. General Requirements. The SECENT training described below meets all mandatory requirements outlined in DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 5 and includes mandatory SECENT-related training for INFOSEC (including CUI), PERSEC, C-InT and OPSEC all under the Wing's IP SETA program focus areas. Distinct types of mandatory training are described below and include initial orientation training, annual refresher training, continuing training, and specialized training.

10.2. Unit SECENT Training. At Yokota AB, unit SECENT training covers the following programs: PERSEC, INFOSEC, CUI, OPSEC, INDUSEC, and C-InT. This training is provided during the initial and refresher training intervals discussed below. Unit commanders task their USM to implement the SECENT SETA program. The USM may require access to unit members' training documentation to validate requirements are completed or coordinate this validation with the Unit Training Manager (UTM).

10.2.1. Initial SECENT Training. There are two types of "initial" training to consider. The "cleared" training applies to members with access to classified information and the "uncleared" applies to those with no access to classified. The training requirements are outlined in DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 5. Both cleared and uncleared training require completion of the DoD Cybersecurity Awareness (AF myLearning CBT) IAW DoD 8570.01M and meets requirements from DoDM 5200.02_DAFMAN 16-1405, DoDI 5200.48_DAFI 16-1403, AFI 10-701 and AFI 16-1402 which covers Cybersecurity, PERSEC, C-InT, CUI, and OPSEC training requirements. Additionally, both categories require annual refresher and continuous education training.

10.2.1.1. Initial SECENT Training for **cleared newcomer personnel** will consist of following:

374 AW Newcomers Orientation

DDo Initial Orientation and Awareness, [Course ID # MLMW2233] in AF myLearning.

Cyber Awareness Course; in AF myLearning.

Derivative Classification Presentation, provided by Unit Security Manager. Member will sign an acknowledgement sheet after review. If newcomer requires access to SIPRNET then completion date will be annotated on DD 2875 by USM.

NATO Awareness Brief: Required by all personnel (military, civilians and contractors) and members who deploy where NATO forces are serving. The USM will conduct this brief and will annotate indoctrination in the member's DISS record. Prior to member's departure the USM will conduct debrief from NATO and annotate accordingly in member's DISS record. If newcomer requires access to SIPRNET then this brief must be given and recorded prior to USM annotating completion date and endorsing the newcomer's DD Form 2875.

10.2.1.2. The USM must document completion of initial cleared training in Database of Record under the non-SCI indoctrination date by verifying completion of the requirements in 10.2.1.1. The USM will also will not sign-off cleared newcomer's inprocessing checklist until verified completion of training requirements.

10.2.1.3. Initial training for uncleared newcomer personnel is required for GS civilians or contractor personnel not authorized access to classified (e.g., a UMD SAR code 8 GS employee). Initial SECENT Training for **uncleared newcomer personnel** will consist of the following:

374 AW Newcomers Orientation

DOD Initial Orientation and Awareness, [Course ID # MLMW2233] in AF myLearning.

10.2.1.4. The USM will validate completion before signing off on uncleared newcomers inprocessing checklist.

10.2.2. Annual Refresher and Continuing Education Training. The SECENT program uses the same method described above to complete annual refresher training. The USM should provide locally produced SETA presentations, slides, e-mails, etc to place additional training emphasis on a quarterly (or more frequent) basis to meet SECENT SETA continuing education training requirements. 374 AW will also provide SETA resources, templates, pamphlets, briefs, to USM that they may use to assist in their unit continuing education efforts.

10.2.2.1. Annual Refresher. The following training courses must be completed on an annual basis by all **cleared** Yokota AB personnel:

Unauthorized Disclosure of Classified Information and Controlled Unclassified Information, [Course ID # MLMW2215]; in AF myLearning.

DOD Mandatory Controlled Unclassified Information Training, [Course ID # MLMW2289]; in AF myLearning.

Derivative Classification Presentation (locally provided by 374 AW/IP via USM).

Insider Threat Awareness Course, [Course ID # MLMW2216]; in AF myLearning.

DoD Annual Security Awareness Refresher, ; in AF myLearning.

DoD Cyber Awareness Course; in AF myLearning.

10.2.2.2. Annual Refresher. The following training courses must be completed on an annual basis by all un**cleared** Yokota AB personnel:

DOD Mandatory Controlled Unclassified Information Training, [Course ID # MLMW2289]; in AF myLearning.

Insider Threat Awareness Course, [Course ID # MLMW2216].

DoD Cyber Awareness Course; in AF myLearning.

10.2.2.3. The USM will ensure the unit method/plan for conducting and tracking annual refresher and continuing education training is reflected in the unit's SECENT OI.

10.2.2.4. The USM must maintain written documentation of who took the training and how/when it was distributed and completed.

10.2.2.5. The USM will verify members have completed the required AF myLearning training. A quarterly (or more frequent) roster from the unit training manager is acceptable.

10.2.2.6. If continuing education training is not conducted by sending out SETA

information quarterly (or more frequently) the USM will outline how the training is accomplished and documented in the unit's SECENT OI.

10.2.2.7. The USM ensures cleared contractors are integrated into the unit's SECENT training program and ensures they complete needed training. The actual training may be conducted by the contractor, USM, or other training personnel. This should be specified in the associated DD Form 254 for the contractor personnel.

10.2.2.8. The USM is responsible to ensure any uncleared contractors assigned to the unit complete required SECENT training per paragraph 10.2.1.3. Documentation of completion will be maintained in the USM continuity binder.

10.2.3. Pre-Deployment Training. The USM will ensure pre-deployment enhanced security training, if required by the unit, is included in the SECENT OI. This training is required for deploying personnel supporting operational contingencies as outlined in DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 5, Section 4.

10.2.3.1. This training should build on the information already included in SECENT Initial/Annual Refresher Training.

10.2.3.2. Ensure any members deploying receive refresher training on INFOSEC. As a minimum include use of NATO information, how to handle/protect US collateral/CUI/foreign government information where foreign allies are present and rules for sharing US information with allies.

10.2.3.3. Ensure all deploying personnel receive mission oriented OPSEC education (i.e. OPSEC Pre-deployment Brief) in accordance with AFI 10-701 (coordinate with unit OPSEC Coordinator). Ensure members are familiar with potential threats related to the organization, critical information for the mission it supports, job specific OPSEC indicators and the OPSEC measures unique to that specific event/AOR.

10.2.4. Documenting/Tracking SECENT Training. The USM is responsible to document and track all required SECENT training. Also:

10.2.4.1. Cleared/Uncleared newcomers training should be completed within 60 days of arrival.

10.2.4.2. The USM must be able to provide proof training, for example a unit training roster with training, names, dates, etc. Computer databases, sign-in rosters which identify topics covered and members who attended from commander's calls/roll call training or e-mail read receipts are acceptable methods of tracking SECENT Annual, Refresher or continuing education training.

10.2.4.3. Initial Cleared Training MUST be completed prior to member accessing classified or CUI. Record initial training for cleared personnel in the "non-SCI Indoctrination" section of the database of record and DD 2875, as applicable.

10.2.4.4. Initial Uncleared Training MUST be completed prior to NIPR access or allowing access to CUI documents. The USM will not sign unit's inprocessing checklist until training completion is validated.

10.3. Derivative Training. Unit commanders identify unit derivative classifiers and ensure they are trained annually IAW DAFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 5, Section

7.c. Volume 3, Enclosure 5, Section 7.c. The USM provides oversight at the unit level and will ensure:

10.3.1. Appointing Derivative Classifiers. A Unit Derivative Classifier Appointment letter signed by the Commander is provided to 374 AW/IP. Do not add derivative classifiers to the letter until required training is complete.

10.3.2. Unit Guidance on Derivative Actions. Any unit specific procedures concerning derivative classification will be outlined in the unit's SECENT OI. At a minimum, include the training/appointment requirements and the fact failure to complete annual refresher training will result in removal from the unit's Derivative Classifiers Appointment letter.

10.3.3. Administrative Items. The USM will provide the 374 AW/IP a copy of the Derivative Classifiers Appointment letter and maintain one in the USM continuity binder. The USM will maintain copies of training records and must be able to provide them upon request (i.e. MAJCOM inspection, Wing CCIP inspection, Wing Annual IP program inspection, etc).

10.3.4. Initial Derivative Classifier Training: Unit personnel who will be appointed as Derivative Classifiers will complete the Defense Counterintelligence and Security Agency (DCSA) web-based courses: Derivative Classification (https://www.cdse.edu/Training/eLearning/IF103/) and the Marking Special Categories of Classified Information (https://www.cdse.edu/Training/eLearning/IF105/). These are the only courses which meet the requirements outlined in of DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 5. Contact your USM if you are having issues accessing the website.

10.3.5. Refresher Derivative Classifier Training. Derivative Classifiers must accomplish derivative refresher training **annually.** The Marking Classified course is a one-time requirement and is not required for the derivative refresher training.

10.3.6. SIPRNET Access. All SIPRNET users are inherently derivative classifiers and the USM will validate required training from **chapter 6** of this instruction is completed prior to annotating completion in block 21 of the DD Form 2875, per paragraph 6.5.2.1. of this instruction.

10.3.7. Oversight. The 374 AW/IP provides oversight by validating completion of training during scheduled inspections.

10.4. Security Container Custodian Training. See paragraph 2.6.4 for requirements.

10.5. Training Requirements for Classified Processing Areas.

10.5.1. Training Requirements. Commanders will ensure USMs work with unit leadership to identify positions in the unit where personnel work in or are authorized access to CPAs. The training will include:

10.5.2. Being developed by the USM, unit training manager and/or section leadership of CPAs to tailor training for the CPA owners.

10.5.3. Inclusion in the unit's SECENT initial and annual refresher training.

10.5.4. Procedures outlined for classified access, as outlined in this chapters 6 and 11.

10.5.5. This training may be included into on-the-job training (OJT)-type training, provided the USM can verify completion, track currency (e.g., has a database) and it has been

reviewed/approved by the 374 AW/IP.

10.6. The 374 AW/IP Training Responsibilities. The 374 AW/IP provides oversight and assists USMs, if requested, in developing localized IP-related SECENT training.

10.6.1. USM Training. As security professionals USMs must complete training outlined in DoDM 5200.01_AFMAN 16-1404, Volumes 1 and Volume 3, to properly perform duties. Commanders should consider setting aside time for USMs to take virtual DCSA CDSE training courses. At a minimum, USMs will:

10.6.1.1. Complete the DCSA CDSE courses as identified in paragraph 2.4.3.5 of this instruction. If USM is appointed additional SECENT positions (i.e. OPSEC Coordinator, Security Container Custodian, etc.), completion of required training for those position will be in accordance with applicable regulation.

10.6.1.2. Attend the USM initial training course conducted quarterly by the 374 AW/IP. Prerequisites apply as stated in paragraph 2.4.3.5 of this instruction.

10.6.1.3. Commanders may request one-on-one USM training on a case-by-case basis if extraordinary situations prevent a USM from attending the quarterly scheduled 374 AW/IP USM training course. Due to amount of time required to conduct the class for one person, this option is only approved on a case-by-case basis with CIP approval.

10.6.1.4. The 374 AW/IP will document USM training with a certificate of completion signed by CIP. A copy will be maintained by the 374 AW/IP and the USM will maintain a copy in continuity binder. The USM is responsible for ensuring this training is documented in any other needed systems (e.g., AF Form 1098, etc.).

10.6.1.5. If a USM fails to accomplish required training within the specified timelines, the CIP will notify the commander the individual is unqualified for USM duty and must be replaced.

10.6.2. Security Officer Visit Admin DISS or successor system NBIS Access. If individuals are appointed by the commander, in writing, they may be granted Security Officer Visit Admin access in DISS or successor system NBIS.

10.6.2.1. The USM will provide a copy of the appointment letter and verify required training is completed with 374 AW/IP PERSEC Specialist.

10.6.2.2. The USM is responsible to maintain copies of applicable training and to ensure currency of the noted courses is also maintained.

10.6.3. Other Specialized Training. The 374 AW/IP is available to assist units in developing unit specific localized IP training plans, upon request. The USM will ensure the 374 AW/IP coordinates on any localized unit training plans covering IP topics (e.g., security container custodian training, derivative training, etc.).

Chapter 11
SECURITY INCIDENTS

11.1. General Information. All personnel will comply with DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 6, when accomplishing requirements for actual/potential compromises of classified information. If possible, report classified security incidents using secure communications. If not, ensure no classified information is passed over unsecure communications creating a security incident in of itself.

11.2. Conducting Incident/Investigation Reports. The commander having responsibility of the individual(s) involved will act as the appointing official (AO) for the inquiry or investigating official (IO). If the individual who would normally act as the appointing official is involved in the incident, the next higher level of command will act as the AO. The report goes directly from the IO to the 374 AW/IP INFOSEC Specialist or CIP and will not to be routed through unit channels prior to Wing IP review. 374 AW/JA review may be requested when incident warrants.

11.2.1. Time Limits. The AO will ensure the IO is appointed within 3-duty days of the initial notification from 374 AW/IP. The required briefings by 374 AW/IP will also be completed within this timeframe.

11.2.1.1. The initial suspense will be established by the 374 AW/IP and will be within 10 duty days of the incident being reported.

11.2.1.2. The CIP may grant up to a 10-day extension on a case-by-case basis. If the IO is prevented or delayed from accomplishing the report for an extended period (e.g., 5 or more consecutive days), the AO should consider reassigning the inquiry to a new IO.

11.2.1.3. The USM will never be appointed as the IO.

11.2.2. Report Format. The IO will use the report format provided by 374 AW/IP INFOSEC Specialist when completing IO reports. Failure to use this format will result in the report being rejected and returned for conformity. IO will properly mark and handle the IO report as CUI, at a minimum.

11.2.3. Statements. Formal statements (i.e., AF Form 1168, *Statement of Suspect, Witness, Complainant*) are not mandatory for inquiries, but will be used when the report is part of an official investigation. Memorandum for Record document can be requested by IO and highly encouraged.

11.2.3.1. When conducting an inquiry, the IO may quote personnel within the body of the IO report and collect statements using a memorandum format via e-mail, memorandum for record, or with an AF Form 1168.

11.2.4. COMSEC-Related Incidents. When a security incident involves COMSEC material, the USM will ensure both 374 CS/SCXSC (225-7009), and 374 AW/IP INFOSEC Specialist are notified. The circumstances and specific information surrounding the incident may be classified; use secure communications or face-to-face means to report.

11.2.4.1. If the situation generates a COMSEC report, a collateral inquiry report is not required.

11.2.5. Inquiry/Investigating Officials. Use DAFI 90-301 as a guideline for selecting inquiry or IOs. Specifically:

11.2.5.1. The IO must be objective, unbiased, and not in the direct chain-of-command of those being investigated.

11.2.5.2. The IO must be of sufficient experience, maturity, have sound judgement and not be less in rank or grade than the person(s) involved with the incident.

11.2.5.3. In order to meet the intent of **paragraph 11.2.5.2** above, as a minimum, IOs must be an officer, E-7, GS-9 or above.

11.3. Incidents with Electronic Devices in Classified Processing Areas. Electronics in classified processing areas represent an extraordinary threat to security.

11.3.1. When a classified security incident involves an unauthorized device, the item will be confiscated and treated as classified (same level as classified involved) until the classified security incident inquiry is complete or until verified it does not contain classified information. Individuals observing the incident will attempt to secure the device from the offender after they report the incident.

11.4. Classified Security Incidents Involving Personal Electronic Devices.

11.4.1. If the USM verifies the personal electronic device did not come within 3 meters of classified systems, no incident will be declared. If this cannot be established, or if the device was within 3 meters, an incident is declared.

11.4.2. If personal electronic devices are involved in a CPA incident, the inquiry official must determine, with advice from JA, IP, WCO and organizational subject-matter-experts (SMEs), whether a classified data spillage to the personal device occurred or if the device represented only a transitory threat.

11.4.3. The USM/CR will assist the inquiry official (IO) in identifying a SME knowledgeable and able to assess if classified information for the area affected is on the device.

11.4.4. For data spills consider the following.

11.4.4.1. SECRET level spills and below, there may be a technology capability to overwrite or sanitize, depending on the device in question.

11.4.4.2. If a device cannot be sanitized, destroy it IAW DoDM 5200.01V3_DAFMAN 16-1404V3, Enclosure 7, Section 6.

11.4.4.3. If an individual refuses to allow the device (government or personal) to be reviewed, contact law enforcement and have them apprehend for failure to obey. In this case, the device will be confiscated by SFs and treated as evidence until the matter is resolved by the inquiry official, SF Investigations, 374 AW/JA and/or OSI.

11.4.4.4. Store affected devices surrendered or confiscated as a classified items until verified as clear of classified.

11.4.4.5. If devices are sent to National Security Agency (NSA) for destruction, follow procedures for mailing classified items.

11.4.4.6. If the device is a government issued item (e.g., cell-phone/two-way radio) and the breach of the zone was momentary while being performed in the course of duties, (e.g., SF responding to unauthorized aircraft run) it is not considered a security incident and does not need to be reported.

11.4.5. Establishing Unit Procedures. Recommend units with CPAs document written procedures in the unit's SECENT OI to ensure personnel are aware of requirements, to include:

11.4.5.1. Clearly identifying CPAs and prohibited devices is critical; here are a few examples of prohibited devices: cellphones (with or without cameras/microphones), flash memory devices, wireless PEDs, MP3 players with record, transmit/flash drive capabilities, etc.

11.4.5.2. Authorization for an item in one CPA DOES NOT automatically allow it into another CPA.

11.4.5.3. Posting visual aids reminding personnel of prohibited devices at CPA entrances. Visual aids for temporary CPAs need only be posted when classified processing is in progress.

11.4.5.4. Clearly identifying devices authorized for use in a CPAs. The procedures must ensure that owning area personnel and security forces (if applicable) are provided a copy of approval letters and a description of the device. Some devices which might be approved for CPA use are EFB iPads, Bluetooth medical devices, etc. In CPAs, these types of devices are ONLY authorized if approved on the TEMPEST package.

11.4.5.5. In the case of Bluetooth medical devices, they are not a risk in CPA where it is only a briefing or review of hardcopy material, so long as the member leaves any linked device (e.g., cellphone or other transmitting device) outside the CPA. In a TEMPEST CPA, these devices will need a TEMPEST review, certified tempest technical authority (CTTA) recommendation, and authorization official (AO) approval before being authorized.

11.4.5.5.1. 374 CS/WCO will process in accordance with TIM 2022-06, DAFGM2024-16-01- and AFSSI 7702, as applicable.

11.4.5.5.2. USM will submit member's request for electronic medical device approval to 374 AW/IP to commence processing.

11.5. CMI/Data Spillage Incidents/NDCI. If classified information is improperly transmitted over unapproved systems, follow the procedures outlined in paragraph 6.6 of this instruction.

11.6. Closing Incidents. Upon final determination of security incident category (i.e. practice dangerous to security, security infraction or security violation) by 374 AW/IP, a closing incident memorandum will be forwarded to AO. The AO will officially close incident with endorsement of memorandum validating corrective actions have been completed or stating non-concurrence with the findings.

11.6.1. Actions if an AO Non-Concurs. An appointing official may challenge all or part of the findings/conclusions but must provide specific reasons in the memorandum. In no case will the IO be required to revise their findings.

11.6.1.1. If the non-concur is reviewed by the CIP and 374 AW/JA (when applicable) and they continue to support the IO's findings/conclusions, the report will be returned to the AO for reconsideration of the original findings.

11.6.1.2. If the AO still non-concurs a second review will be completed of the entire package being reviewed by the 374 AW/CD for final resolution.

Chapter 12
COUNTER-INSIDER THREAT PROGRAM (C-INTP)

12.1. Purpose. This Air Force C-InTP is implemented through this instruction, as a part of the overall SECENT, IAW AFPD 16-14 and DAFI 16-1402.

12.1.1. The C-InTP Concept. The C-InTP is implemented through and managed in conjunction with the SECENT program. C-InTP requirements are integrated into existing programs and specific training is provided for portions of SECENT, through IP annual training, and includes specific C-InTP and continuous evaluation training topics. There is mandatory collaboration between C-InT and PERSEC programs. The C-InTP program ensures:

12.1.1.1. AF personnel are continuously evaluated using enhanced technical capabilities to monitor and audit user activity on information systems.

12.1.1.2. Leveraging the SECENT portfolios associated with Information, Industrial, Operations, and Personnel Security to improve existing installation insider threat detection and taking actions to mitigate noted deficiencies.

12.1.1.3. By integrating and standardizing processes and procedures across the SECENT to help detect, mitigate and respond to insider threats, while ensuring civil liberties and privacy rights are safeguarded.

12.2. C-InTP Governance. The key directives for the C-InTP are DoDI 5200.43, AFPD 16-14 and AFI 16-1402. The 374 AW/IP coordinates with Yokota AB SECENT community (i.e. 374 AW/JA, 374 CS, 374 SFS, 374 FSS, etc) to ensure timely sharing of information to ensure that pertinent information reaches 374 AW/CC and DAF C-InTP personnel so they can take appropriate actions.

12.3. C-InTP Objectives. The overarching goal of the Yokota AB C-InTP is to mitigate the threat represented by insiders through the following objectives:

12.3.1. Network Monitoring and Auditing. This C-InTP function is accomplished through mandated AF Cyber Security actions that are implemented and managed by 374 CS.

12.3.2. Information Sharing. The Yokota AB SECENT community of SMEs includes, but is not limited to: AFOSI, Force Protection, Security Forces Investigations, Wing Cyber Security, Public Affairs and the 374 AW/IP C-InT liaisons.

12.3.2.1. Any derogatory information received by any of these reporting agencies will be shared between offices as required per their regulatory guidance.

12.3.3. Physical Security. This objective is accomplished through on-site reviews conducted by 374 AW/IP, 374 SFS, 374 CS, AFOSI and other applicable functional units/agencies. The goal is to prevent physical access to information. The functional units provide any needed local guidance in their publications and Yokota AB commanders ensure mandated security controls are in place and verify unit members routinely use them to protect assets (i.e., information, people and/or equipment).

12.3.4. Training and Awareness. This objective is accomplished by incorporating C-InTP principles into already existing security training (e.g., SECENT initial/refresher training) to ensure all members are trained and aware of insider threat principles and reporting responsibilities.

12.3.4.1. All Yokota AB military, civilian and assigned contractor personnel are required to complete annual C-InT awareness training. The USM tracks compliance of their unit personnel. The annual requirement can be met by completing Insider Threat Awareness Course, [Course ID # MLMW2216]; in AF myLearning. Also, the USM with 374 AW/IP coordination can create a presentation and use to meet this annual requirement.

12.3.5. Insider Threat Reporting and Response. This goal is met through existing reporting procedures and the noted training IAW DAFI 16-1402 and PACAF/IP C-InT Program Manager guidance.

12.4. Responsibilities. The responsibilities and duties of the Yokota AB C-InTP program are outlined in the guidance of the various agencies that monitor the insider threat. The 374 AW/IP responsibilities are essentially the same as those outlined in chapter 1 of this instruction. Additionally:

12.4.1. Oversight. The 374 AW/CD has general oversight for the Yokota AB C-InTP and executes this oversight through this instruction to ensure the following actions:

12.4.1.1. Development of policy and checklists to provide needed compliance and management oversight for the Yokota AB C-InTP. This is accomplished primarily through this instruction.

12.4.1.2. Identifying and coordinating recommend courses of actions to senior leaders as needed. This will be accomplished through the 374 AW/IP appointed C-InT Liaisons.

12.4.1.3. Coordinating and integrating needed local policy changes which result from changes to the DoD or AF C-InTP. This is done through 374 AW/IP appointed C-InT Liaisons.

12.4.1.4. Written procedures are established as needed. This instruction along with DAFI 16-1402 serve as the base for the written guidance; however, specific agencies may need to develop agency specific guidance on insider threat response.

12.4.1.5. Ensure appropriate CI agencies are notified. Other security agencies will be notified, as authorized, once active investigations are concluded. Ensure 374 AW/IP PERSEC Specialist is notified when final reports of investigations are sent to commanders to ensure proper continuing evaluation notifications are also provided IAW DoDM 5200.02_DAFMAN 16-1405.

12.4.1.6. Ensure notifications are made in a timely manner to potentially impacted security agencies to ensure danger from insider activity is mitigated.

Chapter 13
COMMON ACCESS CARD (CAC) FOR UNCLEARED PERSONNEL

13.1. Policy And Program Management. This chapter establishes guidance for issuance of a CAC to "uncleared" contractor or volunteer personnel in accordance with HSPD-12, DoDM 1000.13, Volume 1, DoDI 5200.46 and DoDM 5200.02. It also locally implements the Mission Partner Identity, Credential and Access Management (MP ICAM) in accordance with DAFMAN 36-3026. The 374 AW/CC appoints the 374 AW/IP as the Yokota AB Installation Point of Contact (IPOC) to manage and oversee the MP ICAM process.

13.2. Duties and Responsibilities. The IPOC implements the Yokota AB MP ICAM program on behalf of the 374 AW/CC through the Mission Partner Affiliate Security Manager (MPASM). The MPASM resides in the 374 AW/IP. Tenant units must comply with Yokota AB MP ICAM program requirements or 374 FSS Military Personnel Flight (MPF) will deny the issue of a CAC to the uncleared personnel.

13.2.1. Mission Partner Affiliate Security Manager (MPASM). The MPASM oversees and manages the Mission Partner Affiliation Sponsors (MPAS). They coordinate and provide required training. They ensure all MP ICAM policy, procedures and requirements are met. They have the ability to initiate a new credential application and complete applications by proxy when the applicant cannot do so due to extenuating circumstances. They ensure issuance of a CAC to uncleared contractors is requested, documented, and tracked through MP ICAM in coordination with MPF.

13.2.1.1. The MPASM maintains the AF program MICT checklists to validate compliance during self-assessments, CCIP events and MAJCOM inspections.

13.2.2. Mission Partner Affiliation Sponsor (MPAS). The MPAS manages and monitors requests and issuance of CACs through MP ICAM. They are responsible for sponsoring the applicant for issuance of a DoD credential for physical and/or logical access or non-DoD credential use for logical access. The MPAS is responsible for managing the complete lifecycle of credential sponsorship. Each 374 AW Group is required to have an appointed MPAS and may further delegate to squadron level.

13.2.2.1. There can be one or more MPASs at a site. A MPAS should not manage more than 100 active applicants without approval form MPASM or unit commander in accordance with DAFMAN 36-3026.

13.2.2.2. Unit commander requiring contractor support will appoint a primary MPAS, in writing, with a copy of the appointment letter provided to the MPASM in 374 AW/IP. The commander should consider appointing at least one assistant but must do so if the primary MPAS's active uncleared contractor population is 100 or more. The MPAS is the most critical part to the MP ICAM program, and it is imperative for them to be fully trained and comply with all duties noted below. The commander and unit MPAS will ensure the appropriate MICT/CCIP checklist is loaded against their MICT/CCIP program to ensure the compliance during self-assessments and IG CCIP events.

13.2.2.3. The MPAS will maintain a continuity book which has a listing of current MPASs (contact information, training completion dates), copies of MPAS training certificates, MPAS appointment letters, MPASM appointment letter and copy of MICT checklist.

13.2.2.4. Commanders are highly encouraged to use their the USM to act as MPASs. This

is due to the fact USMs are already familiar with PSI requirements and have access to the database of record, which can show if an individual already has a “cleared” PSI, alleviating the need to submit a new PSI.

13.2.2.5. If the MPAS is not the USM, the MPAS “MUST” specifically verify with the USM whether or not an applicant already has a suitable PSI for CAC issuance.

13.2.2.6. If a contractor must be submitted for a PSI, the MPAS will ensure the USM makes the needed e-QIP or successor system eApp request. DO NOT approve the individual for a CAC in MP ICAM until the USM confirms the Tier-1 is returned as favorable. If a temporary CAC is needed, see **paragraph 13.3.2** for requirements.

13.2.2.7. Failure to properly execute MPAS duties/responsibilities may be considered abuse of computer systems and/or purposeful violation of security requirements and may result in loss of access to the network and/or classified information.

13.2.3. Actions Required by the MPAS. The unit MPAS will ensure the following actions are accomplished regarding their unit MP ICAM program:

13.2.3.1. Validate the contractor has a requirement for CAC issue against the PWS.

13.2.3.2. Verify contractor has continued affiliation every 180 days.

13.2.3.3. Ensure contractor CACs are revoked in MP ICAM upon termination of affiliation of the contractor or contract.

13.2.3.4. Retrieve CACs upon contractor or contract termination.

13.2.4. Human Resource (HR) Offices. The HR for Yokota AB resides in the CPF and NAF. They will use the already established procedures outlined in **chapter 4** above for submitting, monitoring, and tracking initial-hire, uncleared federal government employees.

13.3. Requirements for PSI. Anyone requiring long-term (6 months or more) access to the installation, an installation facility or the local area network (LAN) is required to have, as a minimum, a Tier-1 investigation. This includes NAF, contractors or volunteers (who require installation entry or LAN access). If there is a conflict between this instruction and a 31- series AFI, the AFI will take precedence.

13.3.1. Installation Entry Only. If an individual already has a valid form of identification for installation entry (e.g., Dependent ID card) and does not require LAN access, IAW DoDM 1000.13, Volume 1, they do NOT require a PSI.

13.3.2. Issuing Temporary CACs. A temporary CAC may be approved for an uncleared contractor by the sponsoring unit commander prior to completion of the Tier-1 ONLY if the FBI fingerprint check has been returned to OPM without derogatory information.

13.3.2.1. If the MPAS is not the USM, they will contact the USM if they need assistance in determining status of the Tier-1 or to get an update on the FBI fingerprint checks for consideration of a temporary CAC. If USMs not available, then MPAS may contact MPASM in 374 AW/IP. The MPAS will NOT make direct contact to DCSA or OPM directly.

13.3.3. If temporary CAC issuance is used for NIPRNET access, the USM will annotate the DD Form 2875 with the following statement, "Temporary CAC authorized IAW DoDM

1000.13, Volume, Enclosure 2, Section 3.b., based on favorable fingerprint check, pending final Tier investigation completion."

13.4. Tracking Uncleared Contractor PSIs. The Central Verification System (CVS) is the system of record for uncleared access PSIs, to include Child and Youth Program (CYP) cases. Although DISS may be used to validate if previous PSI exists, it does not track uncleared cases or show status of uncleared PSIs.

13.4.1. Monitoring Uncleared Contractor PSIs. It is the requesting USM's responsibility to monitor status of and/or request updates to these cases from 374 FSS/FSC. This includes tracking any state repository checks submitted for CYP cases.

13.4.2. Suitability Determinations for Uncleared Contractor PSIs. See **paragraph 4.4.11**.

13.5. Network Access Suspension. See chapter 6 of this instruction for actions to take if network access must be suspended for uncleared contractors.

Chapter 14
OPERATIONS SECURITY (OPSEC) PROGRAM

14.1. Purpose. The Air Force OPSEC program is implemented at Yokota AB through this instruction, as a part of the overall SECENT program, IAW AFI 10-701.

14.2. OPSEC Overview. OPSEC is an information-related capability that preserves friendly essential information by using a process to identify, control and protect critical information and indicators.

14.2.1. OPSEC supports 374 AW and tenant units local planning, preparation, execution and post execution phases of all activities, operations and programs across the entire spectrum of operations. Enhanced operational effectiveness occurs when decision-makers apply OPSEC from the earliest stages of planning. Unit OPSEC Coordinators assist commanders and directors with implementing and practicing effective OPSEC.

14.2.2. OPSEC is a commander's/director's responsibility and is established, managed and implemented at all levels (wing, group, unit, agency, tenant unit, etc.) throughout Yokota AB.

14.2.2.1. Management of OPSEC at Yokota AB resides in the 374 AW/IP (OPSEC Signature Manager) and in each unit/organization/agency (OPSEC Coordinators).

14.3. Roles and Responsibilities.

14.3.1. 374 Airlift Wing Commander will:

14.3.1.1. Appoint in writing, a primary OPSEC Signature Manager at grades no lower than O-3, E-7 or GS-12 and appoint in writing an alternate OPSEC Signature Manager at grades no lower than O-1, E-6 or GS-9.

14.3.1.2. Directs unit-/agency-level OPSEC Coordinators be appointed in all subordinate organizations and on the commander's/director's staff to implement and enhance the effectiveness of OPSEC within the organization and support the Wing's OPSEC Signature Manager.

14.3.1.3. Approve and issue an installation Critical Information and Indicators List (CIIL). Ensure measures are taken to manage signatures, prevent disclosures of critical information and indicators and maintain essential secrecy when warranted.

14.3.1.4. Ensure annual OPSEC inspection/reviews are conducted. These events will be arranged and conducted by the Wing OPSEC Signature Manager in coordination with 374 AW/IP and 374 AW/IG for CCIP events.

14.3.1.5. Ensure OPSEC considerations are included in Yokota AB Public Affairs reviews and all other public information release processes.

14.3.1.6. Ensure contract requirement owners coordinate with OPSEC Coordinators and the OPSEC Signature Manager, the contracting office and other stakeholders to ensure mission critical information and indicators are not placed in publicly available contract documents.

14.3.1.7. Ensure a Wing OPSEC Working Group is established and comprised of unit OPSEC Coordinators.

14.3.1.8. Approve the Yokota AB Annual OPSEC Report; Wing OPSEC Signature

Manager submits report to the HQ PACAF/IP OPSEC Program Manager per AFI 10-701.

14.3.2. Commanders and Directors.

14.3.2.1. Appoint, in writing, an OPSEC Coordinator(s), to enhance the effectiveness of OPSEC within the organization and support the installation's OPSEC Signature Manager.

14.3.2.2. Approves and issues a unit-level CIIL. Ensure measures are taken to manage signatures, prevent disclosures of critical information and indicators and maintain essential secrecy when warranted.

14.3.2.3. Ensure through OPSEC policy letter and training to clearly communicate to unit personnel that the Commander/Director will consider for appropriate disciplinary action all failures to follow directed OPSEC measures/countermeasures and/or any unauthorized disclosure of critical information.

14.3.3. Chief, Information Protection. Provides oversight of the Yokota AB OPSEC Program and serves as the Wing OPSEC Signature Manager.

14.3.4. Wing OPSEC Signature Manager. Serve as the 374 AW commander's representative regarding OPSEC requirements and the point of contact for all Yokota AB OPSEC-related issues between the installation and HQ PACAF OPSEC PM, AF OPSEC Support Team, and all Yokota AB assigned organizations/agencies.

14.3.4.1. Fulfill duties as referenced in AFI 10-701, paragraph 2.22.

14.3.4.2. Chairs the 374 AW OPSEC WG.

14.3.4.3. Leads, plans, and conducts OPSEC assessments, visits and inspections for all Yokota AB organizations and agencies (unless unit has submitted exemption memorandum). Performs as the lead OPSEC representative to the 374 AW/IG for integration into the CCIP process.

14.3.4.4. Develops and maintains OPSEC Policy Letter, OPSEC Implementation Plan and Yokota AB OPSEC Base Profile documents.

14.3.4.5. Authors and submits the 374 AW Annual OPSEC Report IAW AFI 10-701.

14.3.4.6. Submits candidates for the AF OPSEC Course, other OPSEC-related training courses and related events.

14.3.4.7. Establish, maintain, review, and confirms at least annually, the currency of the 374 AW CIIL.

14.3.4.8. Annually, review and assess the effectiveness and efficiency of OPSEC within all organizations and agencies in the 374 AW and tenant units/organizations.

14.3.4.9. Conduct Staff Assistance Visits as requested by subordinate units and tenant organizations for OPSEC program management, planning and assistance in operationalizing OPSEC.

14.3.4.10. Maintains and manages 374 AW OPSEC budget and program expenditures via 374 CPTS.

14.3.5. Unit OPSEC Coordinators will:

14.3.5.1. Fulfill duties as referenced in AFI 10-701, Para 2.24.

14.3.5.2. Complete the required OPSEC training outlined in Chapter 4 of AFI 10-701 and training locally directed by the Wing OPSEC Signature Manager and 374 AW/IP.

14.3.5.3. Conduct OPSEC reviews of organizational documents and photographs in coordination with 374 AW Public Affairs prior to public release, as required.

14.3.5.4. Assist in reviewing unit-related contracting documents to ensure unit CIIL information and indicators are not publically-available in solicitations and other contract-related documents.

14.3.6. 374 Contracting Squadron (374 CONS) will achieve requirements as referenced in AFI 10-701, Para 2.25. 374 CONS OPSEC Coordinators will complete the AFI 10-701, OPSEC training requirements for contracting (i.e. OPSEC and Contracting (CLC-007). Other 374 CONS personnel can and are encouraged to complete this training also as deemed required by 374 CONS/CC.

14.4. OPSEC Working Group.

14.4.1. Concept of Operations: The OPSEC WG is responsible for assisting the Wing OPSEC Signature Manager in the implementation of the Wing's OPSEC Program. The Wing OPSEC Signature Manager will chair the OPSEC WG and will provide status reports directly to the Wing Commander.

14.4.2. This group also oversees the implementation of the OPSEC Program, develops and refines OPSEC plans and addresses emergent or emergency OPSEC program issues.

14.4.3. The OPSEC WG will ensure the timely and efficient review of activities and future plans.

14.4.4. The OPSEC WG will integrate OPSEC into all organization planning and operational processes through collaboration of unit OPSEC coordinators and unit planners as well as other applicable program stakeholders.

14.4.5. The OPSEC WG composition will be unit OPSEC coordinators from each 374 group and squadron. Also, include representatives from PA and AFOSI. Other representatives from other functional units/agencies will be invited to support specialized projects or activities being executed. All members of the OPSEC WG will, at a minimum, possess a SECRET clearance and access to SIPRNet.

14.4.6. The OPSEC WG works in concert with other security/protection-oriented bodies of Yokota AB's SECENT to review security policies for protection of critical information, operations, resources, assets and personnel. It will ensure the timely and efficient examination of the planning, preparation, execution and post execution phases of any activity across the entire spectrum of installation actions and operational environments to include on and off-base (when warranted).

14.4.7. The OPSEC WG will integrate OPSEC into all organization planning and operational processes.

14.4.8. The OPSEC WG standards, guidance and procedures shall be executed pursuant to AFI 10-701, *Operations Security (OPSEC)*.

14.4.9. The OPSEC WG will use the formal OPSEC process as an integral process of force protection to help protect service members, civilian employees, family members, facilities, and

equipment at all locations and in by denying targeted information to terrorists and other adversaries. Since force protection safeguards an organization's most precious asset (i.e. people), it is critical that OPSEC be applied throughout all organizations.

14.5. OPSEC Education and Training. All Yokota AB personnel (military, Department of the Air Force Civilians and DoD Contractors) are required to complete the DAF OPSEC Awareness Training annually through AF myLearning. Additional locally produced OPSEC training can and will be presented by the Wing OPSEC Signature Manager and the Wing OPSEC WG.

14.5.1. Yokota AB Unit OPSEC Coordinators. Unit OPSEC Coordinators will complete initial and refresher training IAW AFI 10-701, and also local training requirements identified in this instruction. Unit OPSEC coordinators must complete the following training courses:

OPSEC Awareness for Military Members, DoD Employees and Contractors; https://www.cdse.edu/Training/eLearning/GS130-signup/

Air Force Identity Management course; https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf

374 AW OPSEC Coordinator Fundamentals course; 1-day course provided by 374 AW Wing OPSEC Signature Manager.

14.6. Evaluating/Inspecting OPSEC. The 374 AW OPSEC Signature Manager, as part of the Installation SECENT and Wing Inspection Team during CCIPs, will inspect every organization annually to verify OPSEC training, policies and procedures are in place to protect critical information and indicators.

14.6.1. All organizations and agencies will utilize the Security Enterprise Management Internal Control Toolset (MICT) checklist to conduct self-assessment on their OPSEC program IAW MICT rules as identified in DAFI 90-302.

14.6.2. Results from OPSEC-related inspections will be loaded into IGEMS and must be addressed and mitigated by the inspected organization.

14.7. OPSEC Requirements Within Contracting and Acquisitions. Organizations requesting contract support will determine and communicate the OPSEC measures required for each contract and ensure they are included in requests for proposal, statements of work, performance work statements, statement of operations, or other contract documents. OPSEC guidance will be levied using DD Form 254 for all classified contracts owned and funded by Yokota AB units/organizations.

14.7.1. Document Reviews.

14.7.1.1. 374 AW OPSEC Signature Managers, in coordination with unit OPSEC Coordinators from the contract requirement owners, are responsible for the review of contract documents to ensure critical information and/or indicators are not made available to the public. An approved Yokota AB CIIL and/or unit CIIL will be used as a reference when conducting reviews.

14.7.1.1.1. The unit OPSEC Coordinator assigned to the unit with the contract requirement conducts the actual review of the contract documents and the 374 AW OPSEC Signature Manager provides technical guidance, if needed, and final approval.

14.7.1.1.2. If it is determined that a contract document contains critical information and/or indicators associated with the performance of the contract, the requesting

organization’s OPSEC Coordinator will develop an OPSEC Plan to protect the critical information and/or indicators associated with the contract from cradle-to-grave if the critical information can’t be removed.

14.7.2. Public Release of Information. The 374 AW OPSEC Signature Manager will work with applicable unit OPSEC coordinators when notified by 374 AW/PA of a need to conduct an OPSEC review for public release of information. If there is a question on whether the information can be released due to FOIA exemptions, the OPSEC official reviewing the information will coordinate with 374 AW/JA for further review and determination.

RICHARD F. MCELHANEY, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DODM 5105.21V1-3, *Sensitive Compartmented Information (SCI) Administrative Security Manual*, 19 October 2012

DoDM5200.01V1 DAFMAN16-1404V1-DAFGM2024-01, *DoD Information Security Program*: *Overview, Classification, and Declassification,* 27 August 2024

DoDM 5200.01V2_AFMAN 16-1404V2, *Information Security Program*: *Marking of Information,* 7 January 2021

DoDM 5200.01V3_AFMAN 16-1404V3, *Information Security Program*: *Protection of Classified Information,* 12 April 2022

DoDM 5200.02_DAFMAN 16-1405, *Department Air Force Personnel Security Program*, 1 August 2018

DoDM5220.22V2_AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, 8 May 20

DoDM 5220.22V2_AFMAN 16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, 8 May 2020

DoDD 4500.54-E, *Department of Defense Foreign Clearance Program,* 31 May 2022

DoDD 5210.50, *Management of Serious Security Incidents Involving Classified Information,*

27 October 2014, Incorporating Change 2, 18 September 2020

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, 6 November 1984, Incorporating Change 2, 15 October 2018

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, 14 April 2004, Certified current as of 23 April 2007

DoD 5200.08-R, *Physical Security Program,* 9 April 2007, Incorporating Change 2, 19 October 2020

DoDI 3305.13, *DoD Security Education, Training, and Certification*, 13 February 2014, Incorporating Change 2, 24 September 2020

DoDI 5200.48_DAFI 16-1403, *Controlled Unclassified Information (CUI), 5 October 2021*

DAFMAN 36-3026, *Mission Partner Identity, Credentialing, and Access Management,* 15 August 2024

AFMAN 14-403, *Sensitive Compartmented Information Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance,* 3 September 2019

DAFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*, 13 September 2022

DAFMAN 17-1302-O, *Communications Security (COMSEC) Operations*, 13 December 2022

AFPD 16-14, *Security Enterprise Governance*, 31 December 2019

DAFI 16-1401, *Information Protection Program*, 3 February 2023

DAFI 16-1402, *Counter-Insider Threat Program Management*, 10 May 24

AFI 10-701, *Operations Security (OPSEC)*, 24 July 2019, incorporating Change 1, 9 June 2020

DAFI 31-101, *Base Defense Operations*, 10 September 2024

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 March 2020

DAFGM2023-36-03, *Suitability/Fitness Adjudication for Civilian Employees*, 14 November 2024

Headquarters, Pacific Air Forces, *Security Classification Guide*, 18 July 2024

Adopted Forms

AF Form 143, *Top Secret Register Page*

AF Form 144, *TOP SECRET Access Record and Cover Sheet*

AF Form 310, *Document Receipt and Destruction Certificate*

DAF Form 847, *Recommendation for Change of Publication*

AF Form 2583, *Request for Personnel Security Action*

AF Form 2586, *Unescorted Entry Authorization Certificate*

AF Form 2587, *Security Termination Statement*

DD Form 1610, *Request and Authorization for TDY Travel of DoD Personnel*

DD Form 2501, *Courier Authorization*

DD Form 2962v1, *Personnel Security System Access Request (PSSAR) Defense Manpower Data Center (DMDC)*

OF 89, *Maintenance Record for Security Containers/Vault Doors*

OF 306, *Declaration for Federal Employment*

SF 85, *Questionnaire for Non-Sensitive Positions*

SF 86, *Questionnaire for National Security Positions (2016)*

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container Information*

SF 701, Activity Security Checklist

SF 702, Security Container Check Sheet

SF 703, *Top Secret (orange)*

SF 704, *Secret Cover Sheet (red)*

SF 705, *Confidential Cover Sheet (blue)*

SF 901, Controlled Unclassified Information (purple)

Abbreviations and Acronyms

AF—Air Force

ADP—Automated Data Processing

AECA—Arms Export Control Act

AFSC—Air Force Specialty Code

AIS—Automated Information Systems

AVS—Adjudication and Vetting Service

AW—Airlift Wing

CAF—Central Adjudication Facility

CCIP—Commander Inspection Program

C-InT—Counter-Insider Threat

CIP—Chief, Information Protection

CMI—Classified Message Incidents

CPA—Classified Processing Area

CPO—Civilian Personnel Office

CPF—Civilian Personnel Flight

CSS—Commander's Support Staff Office

CUI—Controlled Unclassified Information

DCS—Defense Courier Service

DEFCON—Defense Condition

DISS—Defense Information System for Security

DNI—Director of National Intelligence

EAL—Entry Authority List

EMSEC—Emission Security

EO—Executive Order

EOC—Emergency Operations Center

EPL—Evaluated Products List

e-APP—Electronic Application under NBIS

INDUSEC—Industrial Security

INFOSEC—Information Security

IO—Inquiry Official

IPOE—Intelligence Preparation of the Operational Environment

ISOO—Information Security Oversight Office

JPAS—Joint Personnel Adjudication System

NBIS—National Background Investigation Services

NSA—National Security Agency

OCA—Original Classifying Authority

OPSEC—Operations Security

OPM—Office of Personnel Management

OSA—Open Storage Area

PERSEC—Personnel Security

PDT—Position Designation Tool

PR—Periodic Reinvestigation

PSI—Personnel Security Investigation

SAC—Special Agreement Check

SAP—Special Access Program

SAR—Security Access Requirement

SCG—Security Clearance Guide

SCI—Sensitive Compartmented Information

SETA—Security Education and Training Awareness

SIF—Security Information File

SOR—Statement of Reason

SSBI—Single Scope Background Investigation

SSO—Special Security Officers

TSCA—Top Secret Control Accounts

TSCO—Top Secret Control Officers

TWG—Threat Working Group

U.S.—United States

USD(I)—Under Secretary of Defense for Intelligence

USM—Unit Security Manager

USPS—United States Postal Service

WCO—Wing Cybersecurity Office (374 CS/SCXS)

Attachment 2
EMERGENCY PROTECTION, REMOVAL AND DESTRUCTION OF CLASSIFIED MATERIAL PLAN TEMPLATE

A2.1. Template for Emergency Plan. Unit Emergency Plans should be established using this attachment as well as guidance provided by template in DoDM 5200.01V3_DAFMAN 16-1404V3, Appendix 2 to Enclosure 2. However, unit emergency plans must be direct and specify exactly how assigned personnel must react in an emergency.

A2.2. Threat.

A2.2.1. Natural Disasters. Natural disasters may include earthquakes, typhoons, heavy rains, snow, etc.

A2.2.2. Civil disturbances, terrorism, and enemy actions. YAB is susceptible to civil disturbances from outlying communities. Terrorism is a threat that could be experienced at any military installation at any time. The threat of terrorist action increases with the level of the local Force Protection Condition (FPCON).

A2.2.3. Limiting Factors. The 374th Communication Squadron's SCXK Flight manages the Central Destruction Facility (CDF) for the base, located in building #4350, which houses a SEM disintegrator (mechanical pulverizer). For routine use and training, contact 374 CS/SCXK at 225-8205. This single CDF is not capable of destroying all classified material within the time criteria specified by this plan. As a result, units must effectively plan and acquire enough routine and emergency destruction equipment to execute this plan.

A2.3. Execution.

A2.3.1. PHASE I, Emergency Protection. Phase I will be implemented in the event of fire, natural disaster, bomb threat, civil disturbance, or in the case of an increased terrorist threat.

A2.3.1.1. Fire, Natural Disaster, or Bomb Threat.

A2.3.1.1.1. Secure material in approved security containers if time and safety permit. When personal safety is jeopardized, evacuate the area and post individuals *(who you will direct to take care of this action; how will they secure the facility, emergency notifications to Security Forces if needed, etc.?)* to control entry and emergency access (owner/user are responsible for the protection of their classified and facilities, Security Forces will not be used to perform this function).

A2.3.1.1.2. Allow only first responders to enter the facility (Fire Department, Medical Services, Security Forces, etc.). Classified custodians may enter the facility to account for the unsecured classified materials once the area has been declared safe by the on-scene commander. *(What actions do you want the custodians to perform after the area is declared safe, i.e., ensure classified is accounted for; report missing classified, report damage, debrief emergency personnel when they inadvertently review classified materials, etc.)*

A2.3.1.1.3. No entry to the facility will be allowed, until all classified material is accounted for *(how will you accomplish security of the building until the area is declared safe?)*.

A2.3.1.2. Civil Disturbance or Increased Terrorist Threat.

A2.3.1.2.1. Post personnel in classified storage areas *(specify what classified storage areas people will be posted and the actions they need to take, etc.)*, if the situation warrants. Posted personnel must be knowledgeable of procedures to request emergency assistance. Armed guards are not required.

A2.3.1.2.2. Prepare for the initiation of Phase II. Phase II is implemented when the possibility of conflict increases.

A2.3.2. PHASE II, Precautionary Destruction.

A2.3.2.1. Segregate all classified into "mission essential" and "non-mission essential" categories.

A2.3.2.2. Retain mission essential classified material. Destroy non-mission essential classified material using authorized destruction methods *(specify where the material should be destroyed, locations of shredders, if destruction receipts are required, etc.)*.

A2.3.2.3. Prepare for PHASE III. Emergency Destruction.

A2.3.3. PHASE III, Emergency Destruction.

A2.3.3.1. PHASE III actions will be initiated upon the determination an imminent threat exists of the installation being overrun. The effect of premature destruction is considered inconsequential when measured against the compromise of classified information. Emergency destruction may only be declared by the Commander, 374th Airlift Wing.

A2.3.3.2. Each unit will predesignate *(let assigned personnel know where the unit's predesignated location will be)* a location for the emergency destruction of classified material and procure or manufacture sufficient means to accomplish the destruction process (i.e., modified trash cans, BBQ grill, etc.) *(all of these materials should be purchased and on-hand in the event of an emergency—USMs should ensure personnel know where the supplies are stored, etc.)*. If time does not permit you to use predesignated material, immediate destruction will be accomplished in any available container.

A2.3.3.3. Top Secret material holders must have the capability to destroy all holdings within one hour.

A2.3.3.4. Secret and Confidential material holders must destroy the materials within two hours.

A2.3.3.5. No destruction records are required under emergency destruction procedures.

A2.4. Notification.

A2.4.1. The 374 AW Command Post will implement this plan by order of the installation commander or higher authority.

A2.4.2. The 374 AW Emergency Operations Center (EOC) will likely be formed during situations warranting implementation of any destruction phases and will ensure all units are notified as well as track progress *(who are the designated EOC representatives, who are the designated UCC members; what do you want them to do, who and how do they report, how do you get hold of them, etc.)*.

A2.4.3. Any senior individual present in an area containing classified material that determines there is a sufficient threat, may implement any portion of this plan.

A2.5. Preparation Instructions.

A2.5.1. Assign classified material one of the following priorities.

A2.5.1.1. Priority One: TOP SECRET.

A2.5.1.2. Priority Two: SECRET.

A2.5.1.3. Priority Three: CONFIDENTIAL.

A2.5.2. **(Develop in-depth checklists to implement this plan)** Post the checklists in the first file of the security container-locking drawer or on the primary entrance to OSA, and bulk storage rooms.

A2.6. Taskings. *(This section is only a guide--this is where you can list the tasks you want your people to accomplish)*

Attachment 3
CLASSIFIED MEETING CHECKLIST

Table A3.1. Checklist for Classified Meetings derived from DoDM 5200.01V3_DAFMAN 16-1404V3, Appendix 1 to Enclosure 2.

Classified Meeting Checklist				
The security assistant is responsible for ensuring all items below are accomplished, unless the commander or director has delegated the responsibility to another individual. *Note: In this instance, "meeting" encompasses briefings, conferences, etc.*				
#	Preparation Checks	Complete		Comments
		Yes	No	
1	Determine the highest level of classification to be disclosed, to include any additional access requirements			
2	Determine meeting location (e.g., USG or cleared contractor facility) Be sure to select a meeting location that provides good physical control of the meeting room and provides protection from unauthorized audio and visual disclosure			
3	Determine if entire meeting will be classified or if there will be unclassified breakout sessions			
4	Determine where classified material will be stored before, during and after the meeting and who will be responsible for managing it; this includes determining if classified note taking will be permitted and storage/distribution protocols			
5	Identify potential attendees; this includes determining if foreign nationals/representatives will be in attendance. If so, arrange for a disclosure review, of unclassified and classified information, from the foreign disclosure office			
6	Ensure a visit authorization request is submitted, for each attendee, in DISS (or successor system), to verify security clearance eligibility and establishment of need-to-know			
7	Establish a method to identify attendees for entry/reentry (e.g., control rosters, badges, etc.) into the meeting			
8	Establish a screening process for personal items (e.g., briefcases, backpacks, purses, etc.) to prevent unauthorized items from entering the meeting			
9	Identify information systems or audio equipment to be used and ensure it is authorized for classified disclosures			
10	Identify any special communication requirements (e.g., secure terminal equipment), if required			
#	Pre-meeting Inspection	Complete		Comments
		Yes	No	
1	If unfamiliar with building (meeting location), request the building manager be present while conducting walkthroughs			
2	Conduct a visual check of walls, ceilings, and floors for suspicious objects, accessible areas (e.g., holes, openings, exposed wires, etc.)			
3	Ensure all doors, windows and other openings are closed before disclosing classified information; first-floor windows and windows on doors must be covered to prevent visual disclosure; and windows on other floors that allow visual disclosure must be covered			
4	Check, touch and lift (if possible) the following items for things out of the ordinary (e.g., recording devices): Trash			

Table A3.2. Checklist for Classified Meetings derived from DoDM 5200.01V3_DAFMAN 16-1404V3, Appendix 1 to Enclosure 2.

	containers, fire extinguishers, tables, desks, chairs, curtains, pictures, and circuit breaker panels			
#	Before/During the Meeting	Complete		Comments
		Yes	No	
1	Post appropriately cleared DAF personnel outside the meeting area, place signage on the doors, and/or lock entrances to control access			
2	Conduct sound checks to ensure conversations cannot be heard by un-cleared personnel outside the meeting area			
3	Conduct checks of personal items and look for unauthorized, unusual or suspicious items; if an attendee denies the inspection, the item shall not accompany the attendee past the entry control point			
4	Ensure portable electronic devices are not brought into areas where classified information is disclosed			
5	If classified note taking is permitted, brief attendees on the proper safeguarding and marking requirements prior to the start of the meeting			
6	Always announce the highest level of classification for each session			
7	Remind attendees that classified information cannot be discussed freely once the meeting is finished and discussions outside the designated area are prohibited			
8	Ensure all classified meeting material is properly marked and the appropriate coversheets are being utilized			
9	Employ procedures to protect classified material during any type of break, by establishing procedures for protection and storage of classified material at all times			
10	Revalidate all attendees upon reentry from breaks			
#	After the Meeting	Complete		Comments
		Yes	No	
1	Check all areas for unattended classified or unauthorized items left behind by attendees			
2	Notify the activity security manager or servicing information protection office of any security incidents			
3	Turn facility back over to facility manager, if required			
4	Ensure all classified material is secured in an authorized security container			
5	Ensure completed checklist is signed and dated			

Meeting Point of Contact	Signature	Date

Attachment 4
UNIT SECURITY MANAGER APPOINTMENT LETTER TEMPLATE

Figure A4.1. Template for Unit Security Manager Appointment Letter.

CUI
DEPARTMENT OF THE AIR FORCE
374TH AIRLIFT WING

DATE

MEMORANDUM FOR 374 AW/IP

FROM: UNIT/CC

SUBJECT: Appointment of Unit Security Managers

1. In accordance with DoDM 5200.01V1_DAFMAN 16-1401V1, paragraph 7(a)(1), the following personnel are appointed unit security managers as designated (primary/alternate) below for the UNIT:

RANK/NAME	OFFICE SYMBOL	PRI/ALT	DEROS	PHONE
TSgt Aim B. High	374 ???/???	Primary	31 Jun 26	225-4321
SSgt Me B. Fly	374 ???/???	Alternate	25 May 27	225-1234

2. This memorandum supersedes all previous memos of the same subject.

3. Please direct any questions to ONE OF THE SECURITY MANAGERS LISTED ABOVE.

COMMANDER, RANK, USAF
Commander

Controlled by: USAF // 374 AW/IP
CUI Category: OPSEC
Limited Dissemination Control: FEDCON
POC: Chris Turner, Sr., GS-12, 225-8361

CUI

Attachment 5
UNIT SECURITY CONTAINER CUSTODIAN APPOINTMENT LETTER TEMPLATE

Figure A5.1. Template for Unit Security Container Custodian Appointment Letter.

CUI

DEPARTMENT OF THE AIR FORCE
374TH AIRLIFT WING

<DATE>

MEMORANDUM FOR <UNIT NAME>
374 AW/IP

FROM: <UNIT CC>

SUBJECT: Security Container Custodian Appointment Letter

1. In accordance with DoDM 5200.01v3_DAFMAN 16-1404v3, enclosure 3, paragraph 10c, the following personnel are appointed as the Security Container Custodians for the following safes and/or vaults:

Safe Number	Building	Room

Duty Position	Rank / Name	Unit	Phone Number	DEROS

2. Security Container Custodians are to assist the Unit Security Manager(s) as required. Any questions or comments concerning the appointments can be directed to the above personnel or the <UNIT SECURITY MANAGER NAME(s)>

3. This letter supersedes all others on the same subject and is effective immediately.

<CC Name, Rank, USAF>
<Commander>

Controlled by: USAF// Your Unit
CUI Category: OPSEC
Distribution/Dissemination: FEDCON
POC: Your Name, Rank, DSN: 315-225-xxxx

CUI

Attachment 6

CHECKLIST FOR USE OF COPIERS/SCANNERS WITH SENSITIVE INFORMATION CHECKLIST

Table A6.1. INFOSEC Checklist for use of copiers/scanners with sensitive information.

USE OF COPIERS/SCANNERS WITH SENSITIVE INFORMATION

INFOSEC CHECKLIST		**PAGE 1 OF 2 PAGES**		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA **Unit Purchase/Use of Classified Copiers or Scanners references are to DOD 5200M.01 & DoDM 5200.01V3-AFMAN 16-1404V3**		**OPR** **374 AW/IP**	**DATE**	
NO	**ITEM**	**YES**	**NO**	**N/A**
1	The following checklist was developed by the 374 AW/IP using the noted references. You must contact your USM to ensure all requirements for your classified copier or scanner are properly addressed in your unit's local procedures. USM should also contact 374 CS/SCXS (WCO) for applicable Cybersecurity requirements.			
2	Are classified copiers/printers/scanners clearly identified, to include: a. Having a copy of the commander's designation/approval letter which includes the device manufacturer and model, posted near the device? [REF: DoDM 5200.01V3_AFMAN 16-1404V3, E2, Section 14.] b. Has the equipment received TEMPEST approval from the WCO, and been coordinated through the Unit CSR, to include number of blanks needed to clear latent images? [REF: DoDM 5200.01V3_AFMAN 16-1404V3, E2, 14—inclusive.] c. Have procedures been developed and posted near the device which address copying, clearing, control, individual security responsibilities and who is authorized to reproduce classified material [e.g., CC policy letter or in unit OI)? [REF: DoDM 5200.01V3_AFMAN 16-1404V3, E2, 14.b.] d. Is a "Cleared for Classified" sign and equipment marked with SF 706, SF 707, SF 708, SF 710, as applicable, posted at the device? [REF: DoDM 5200.01V3_AFMAN 16-1404V3, E2, 15.b(7).] e. IF the device is connected/part of an Information Technology (IT) system (i.e. a networked e-device), is the equipment marked with the SF 706, SF 707, SF 708, SF 710 as applicable? [REF: DoD 5200.1M Vol 2, Enclosure 3, 18. g(1).]			
3	Classified devices: a. Received Certification and Accreditation (C & A) if connected to a network? [REF: DoDM 5200.01V3_AFMAN 16-1404V3, E2, 14.e.]			

Table A6.2. INFOSEC Checklist for Use of Copiers/Scanners with Sensitive Information.

INFOSEC CHECKLIST		**PAGE 2 OF 2 PAGES**		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA Unit Purchase/Use of Classified Copiers or Scanners references are to DOD 5200M.01 & DoDM 5200.01V3_AFMAN 16-1404V3		**OPR 374 AW/IP**	**DATE**	
NO	**ITEM**	**YES**	**NO**	**N/A**
	COPIER/SCANNER RULES FOR TS MATERIAL			
4	Units possessing large repositories of TS must have a TS Control Program and a designated TS Control Officer (TSCO.) The TSCO must authorize and log any TS copies a unit produces. Specific TSCO requirements may be obtained from the unit security manager and 374 AW/IP.			
5	TS CONTROL- Is the proper annotation made on the AF Form 143, TS Register Page when copies of TS information are made? [REF: DoDM 5200.01V1_AFMAN 16-1404V1]			
6	TS CONTROL- Does the AF Form 143 reflect the following: a. Sufficient information to adequately identify the TS document or material; to include title or appropriate short title, date of the document, and the originator's identity? b. The date the document or material was received? c. The number of copies received and/or later reproduced? d. The disposition of the TS document or material and all copies of such documents or material? e. Are register pages with active entries recontrolled on an annual basis? (AF Form 143) [REF: DoDM 5200.01V1_AFMAN 16-1404V1]			
7	TS CONTROL- Is an AF Form 144, *Top Secret Access Record* and Cover Sheet, attached to each copy of the TS document? [REF: DoDM 5200.01V1_AFMAN 16-1404V1.]			
8	TS CONTROL-Are TS facsimiles processed as another copy of the main TS document in the TS registry? [DoDM 5200.01V1_AFMAN 16-1404V1]			

Attachment 7

ELECTRONIC FLIGHT BAG (EFB) PROGRAM

The EFB Program is a supplement to operations of the 374th Airlift Wing and mission partners; the program allows for approved unclassified electronic devices to enter into classified areas to perform duties necessary to support the mission of all flight crews. Authorized users of the EFB program are required to coordinate with the custodians of the classified processing area (CPA) prior to entering the area.

A7.1. Roles and Responsibilities.

A7.1.1. EFB Program Manager (PM) is assigned within the 374th Operations Group:

A7.1.1.1. Establishes EFB Program rules of engagement and procedures; coordinates with the 374 AW/IP and 374 CS to ensure compliance with directives and policy.

A7.1.1.2. Creates necessary documentation to properly deploy the EFB devices into the classified spaces.

A7.1.1.3. Provides training for proper EFB device use and configuration; coordinates with 374th CS about best practices and compliance to device configuration.

A7.1.1.4. Maintains proper documentation / chain of custody for EFB devices.

A7.1.2. CPA Owner / Custodian:

A7.1.2.1. Oversees the EFB compliance for use within respective CPA.

A7.1.2.2. Validates the EFB devices are configured correctly to meet the standards of the AF 4170.

A7.1.3. Authorized User:

A7.1.3.1. Utilizes EFB in CPAs in order to support the mission.

A7.1.3.2. Receive authorized government EFB from 374 OG/PM; maintains ownership and control until the EFB is turned in.

A7.1.3.3. Comply with EFB/CPA checklist prior to entering CPA.

A7.1.3.4. EFB user is issued properly configured government EFB from the 374th OGV; maintains ownership, control, and latest software of the device until the EFB is turned in.

A7.2. Authorized Areas.

A7.2.1. 374 OG Intel/Tactics Vault – Building 703; third floor

A7.2.2. 374 OG WAR Room – Building 703; Room 212

A7.2.3. 459 Briefing Room – Building 702; Room 207

A7.2.4. 36 AS Tactics Vault – Building 602; Room 213

A7.2.5. 36 AS Briefing Room – Building 602; Room 214

A7.2.6. 36 AS Unit Control Center (UCC) – Building 602; Room 223

A7.2.7. 374 OSS C130J Flight Simulator Facility – Building 912

A7.2.8. Command Post Basement – Building 315

A7.2.9. Wing Command Section – Building 315; Room 212, 213, SIPR/Conference Rooms

A7.2.10. 374th CS Mission Defense Team (MDT) Vault – Building 653

A7.2.11. 374th CS Network Control Center (NCC) – Building 653

A7.2.12. AFSOC CPA Locations

A7.2.13. USFJ / 5th AF CPA Locations – Building 714

A7.3. Documents.

A7.3.1. Risk assessment/AF Form 4170 – document that assesses the potential risks to compromise of classified information based on the location of the classified area. On the approved list of devices, the EFB device(s) will be stated. 374 CS maintains the forms for each CPA.

A7.3.2. Authorization Log – document that tracks the EFB while it is within a CPA; the log's columns should have a date, EFB Authorized User, initial, verifier name, time in and time out (refer to A4.5 Authorization Log Example). The Authorization Log is subject to inspection.

A7.3.2.1. Authorization Log will be placed at the entrance of the CPA.

A7.3.3. EFB CPA Checklist – checklist used to configure the EFB prior to entering the CPA. It is placed in the gap between the EFB device and the cover once it is completed to indicate the device has been configured (refer to A6.7. Diagram of Orange Checklist).

A7.4 Procedure.

A7.4.1. The EFB devices are issued out by the 374 OG; at the time of issuance, the user must request for authorization to take the EFB in a CPA listed in paragraph A6.2 "Authorized Areas."

A7.4.2. Authorized users coordinate date and time with owner of the CPA or custodian.

A7.4.3. Prior to entry into the CPA, authorized user configures the EFB device; instructions are located on the EFB CPA Checklist.

A7.4.4. The CPA owner or custodian verifies the EFB device configurations to match the EFB CPA Checklist; signs as the verifier on the Authorization log.

A7.4.5. Authorization log is filled out by the Authorized user and verifier.

A7.4.6. While in the CPA, EFB devices are not allowed to be left unattended. Additionally, users will configure the device to inhibit all wireless modes. When wireless is inhibited, the MAF EFB can be operated with a minimum of 5 cm separation from classified processing equipment. When the EFB is connected (charging via an approved power receptacle), separation must be a minimum of 1 meter from classified processing equipment. The inhibiting of the camera function and microphone must also be ensured.

A7.4.7. After EFB device exits the CPA, authorized user and verifier annotate the "Time Out" on the authorization log.

A7.5 Contacts for Further Discussion

A7.5.1. Direct all specific questions or concerns to the 374th AW EFB Program Managers at 374ogv.ogv2@us.af.mil and 374 AW/IP at 374AW.IP.Office@us.af.mil.

References:

ACC Instruction 11-270, Operations Mobile Devices (OMDS), 6 November 2024

PACAF/CD Memorandum, 30 December 2019, Electronic Flight Bag (EFB) Usage in PACAF-Controlled Classified Processing Areas

AMC/A3 MAF EFB CONEMP, 28 October 2015, MAF EFB Concept of Employment, https://eim2.amc.af.mil/org/a3v/EFB/default.aspx

AFNIC Memorandum, 10 May 2013, MAF EFB Usage in CPAs

AMC/DA7 Memorandum, 15 April 2013, Use of MAF EFB in MAF Aircraft Simulators Designated as CPAs.

A7.6. Authorization Log Example.

Electronic Flight Bag (EFB)

Classified Processing Area (CPA) Log

Unit Name: **Bldg:** **Room:**

DATE	EFB Authorized User (Last, First)	Initials	Verifier Name (Last, First)	Initials	Time In	Time Out

Figure A7.1. Diagram of Orange Checklist.

Attachment 8
INFORMATION/PHYSICAL SECURITY STANDARDS FOR CLASSIFIED PROCESSING AREA

Table A8.1. Information/Physical Security Standards for Classified Processing Area (CPA) Checklist.

Information/Physical Security Standards for Classified Processing Areas (CPA) Checklist for Site Survey				OPR: 374 AW/IP		
Unit	Building #	Room #	374 AW/IP Surveyor:		DATE:	
				YES	NO	N/A
1	**Classified Processing Areas (CPA) Standards IAW DoDM 5200.01V3_ DAFMAN 16-1404V3**					
a	Are the walls, floors and roof construction of permanent construction material, (i.e. plaster, gypsum, wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance and/or preventing unauthorized entry into the area.)					
b	If present, are windows covered with material that will provide protection unauthorized viewing? (i.e. blinds, curtains, frosting)					
c	Does room have a GSA-approved security container for storage of classified hard drive, laptop, TACLANE key and other classified documents?					
d	If yes, is there a Security Container Custodian appointment letter completed?					
e	Does door have a manual locking device, cipher lock and/or electric lock to control access during active classified information processing?					
f	Is computer screen in direct sight of room entrance door? (NOTE: must not be viewable from the entrance door)					
g	Has the room been EMSEC approved by Wing Cybersecurity Office (WCO)?					
h	Are Unit SOPs developed to ensure continuous monitoring/positive control of classified information during active CPA? (Developed locally)					
i	Is voice (speech) recognizable outside of room? -- Potential Mitigations actions: Stand-off distance/white noise/Music outside of room to mask voice conversations.					
j	Are there any Host Nation work areas inside the proposed CPA?					
k	Is there a classified printer in room? If so, is there an NSA-approved cross-cut shredder present? If not, are proper courier bags available for safeguarding of classified documents?					
l	Has an Emergency Action Plan (EAP) been created to address destruction or safeguarding concerns during emergency events? (Note: Provide recommended posting location of EAP & SOP to USM)					