BY ORDER OF THE COMMANDER
8TH FIGHTER WING

8TH FIGHTER WING INSTRUCTION
16-1404

5 NOVEMBER 2024

Operations Support

AIR FORCE INFORMATION SECURITY PROGRAM

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: 8FW/IP

Certified by: 8FW/CC
(Col Peter E. Kasarskis)

Supersedes: 8FWI16-1404, 14 January 2016

Pages: 19

This instruction enhances Department of Defense Manual (DoDM) 5200.01_AFMAN 16-1404, Vol 1-3, *Information Security Program;* DoDM 5200.2_AFMAN 16-1405_AFGM 2022-03 *Air Force Personnel Security Program*, DoDM 5220.22_AFMAN 16-1406V2 *National Industrial Security Program*, and Air Force Instruction (AFI) 16-1402, *Counter-Insider Threat Program Management* for the 8th Fighter Wing (8 FW). This instruction defines the responsibility and procedures for managing the 8 FW's Information Protection Program. It applies to all assigned, attached, and associated units to the 8 FW, Kunsan Air Base (AB), Republic of Korea. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route the AF Forms 847 from the field through the appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with (IAW) Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This revision incorporates the DoDM5200.01_AFMAN 16-1404, Vol 1-3, ISP requirements to include renumbering paragraphs; and updating/deleting paragraphs and publication references. This document has some minor changes to include: The delegation of the Information Protection

program oversight, the deletion of the ISP Assistant designation, deletion of Location Information Protection Management Evaluations (LIPME), designation of the 8 FW's Annual Classified Clean Out Day, modification of the usage of AF Form 2583, *Request for Personnel Security Action*, modifications to **Attachment 4**, *Security Assistant Appointment Memorandum Template*, and deletion of *Semiannual Self-Assessment Template* attachment.

1. Program Management: The 8 FW Deputy Commander is delegated the duties and responsibilities associated with the oversight of the 8 FW's Information Protection program as outlined in DoDM 5200.01_AFMAN 16-1404, Vol 1-3, Information Security Program. The 8 FW Information Protection (8 FW/IP) office provides oversight for organizations participating in the Information, Personnel, and Industrial Security programs at Kunsan AB, Republic of Korea

1.1. Tenant units declining participation in the Information, Personnel, Insider Threat, and Industrial Security programs by not selecting the Information Protection field in the DD Form 1144, *Support Agreement*, must establish a Memorandum of Agreement (MOA) with the 8 FW/IP office if support is requested. Units requesting waiver from 8 FW/IP oversight should have their Major Command (MAJCOM), Direct Reporting Unit (DRU), or Forward Operating Area (FOA) commander who possesses security Administrative Control (ADCON) author an Information Protection Program Waive out Memorandum (**Attachment 2**.)

1.2. The 8 FW Command Post is designated as the overnight storage repository for United States (US) and North Atlantic Treaty Organization (NATO) classified material in the possession of transient personnel. Repository custodians will develop written procedures for accountability and storage of transient classified materials.

1.3. All Korean Foreign Nationals (KFNs) employed by the 8 FW are required to have an employment background check completed prior to their start date. Favorable completion of the United States Forces Korea Regulation (USFKR) 190-7, *Installation Access Control*, and United States Forces Korea (USFK) Form 82-E, *Application for Installation/Base Pass*, is the Host Nation "equivalent" to a National Agency Check with Written Inquiries (NACI) for KFNs. The date of the KFN employee's last favorable background investigation is listed on the back of the employee's USFK 37-EK, *Installation/Base Pass* and is valid for three years.

1.3.1. Pursuant to USFK 190-7, USFK Form 82-E does not grant KFN access to classified materials, classified computer systems or Protection Level (PL) 1/PL 2 resources as defined in DAFI 31-101, *Integrated Defense (CUI)*. If a KFN job description requires access to classified information or PL 1 or PL 2 resources the owning unit commander must process a Limited Access Authorization (LAA) according to DoDMAN5200.02_AFMAN16-1405.

1.3.2. Approved USFK Form 82-E are maintained by the 8th Security Forces Squadron (8 SFS), Pass and Registration section.

1.4. Contractors performing work at Kunsan AB who require a Common Access Card (CAC) Identification (ID) must be properly vetted in accordance with Homeland Security Presidential Directive - 12 and DoDI 5200.46, *DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)*, prior to issuance. When new contractors arrive or reissuance of a CAC ID is required due to a contract extension/renewal, contractors are required to complete the *In-Processing Checklist for Contractor Requiring a CAC ID* (**Attachment 3**)

1.5. The second Wednesday in April and October is designated as the 8 FW's Annual Classified Clean-out Day. Commanders are responsible for ensuring specific attention and effort are placed on properly disposing of unneeded classified material (documents, CD/DVD. IT equipment, etc.) within their organization.

1.6. Kunsan Theatre is authorized for large, classified briefing such as the following:

1.6.1. Newcomers Briefing (Korea Readiness Operation (KRO) Intelligence (Intel) and Office of Special Investigations (OSI) Briefing). The 8 FSS Security Assistant is responsible for managing the meeting unless the Commander delegates responsibility to another individuals.

1.6.2. Commander Classified All Calls. The 8 Wing Staff Agency (WSA) Security Assistant is responsible for managing the meeting unless the Commander delegates responsibility to another individual.

1.6.3. Wing Pilot Verification. The 8th Operations Support Squadron (8 OSS) Security Assistant is responsibility for managing the meeting unless the Commander delegated responsibility to another individual.

2. Information Security: The goal of the unit's information security program is to ensure classified and controlled unclassified information is protected from unauthorized access.

2.1. Unit commanders are responsible for:

2.1.1. LEVEL 2 SUB-SECTION: Notifying 8 FW/IP, in writing, when a new primary or alternate Unit Security Assistant (SA) is appointed (**Attachment 4**). Commanders will only appoint SAs with more than 6 months' time left on station. Ideally, commanders must allow 7 days of overlap between the incoming and outgoing Unit SA.

2.1.2. Ensuring Primary SAs are in the grade of E-5/SSgt and above while Alternate SAs are in the grade of E-4/GS-5 and above. In addition to an on-line prerequisite course, SAs will receive formal training from 8 FW/IP.

2.1.3. Ensuring initial approval requests for classified vaults, secure rooms, or open storage areas include an inspection by 8 FW/IP, 8 CES Structural Office and Alarm Shop, and 8 SFS Physical Security. In cases of classified electronic processing equipment, 8th Communications Squadron Emission Security (8 CS/EMSEC)-TEMPEST will be included during the initial physical security survey.

2.1.4. Identifying unit derivative classifiers and/or classified Information Technology (IT) system users in writing by signed memorandum. Personnel identified as derivative classifiers and/or classified IT system users must complete Derivative Classification training annually.

2.2. Unit security assistants are responsible for:

2.2.1. Ensuring a copy of the unit's Emergency Protection, Removal, and Destruction Plan is near each security container and inside any approved open storage room/vault. Units may use the 8 FW's Emergency Protection, Removal, and Destruction Plan (**Attachment 5**) to develop unit specific instructions.

2.2.2. Contacting their respective unit's 3D0X1 representative to determine if their classified reproduction equipment has latent image clearing capabilities. All classified copiers must have local instructions posted on/near the copier.

2.2.3. Issuance of DD Form 2501, *Courier Authorization*, or a courier authorization memorandum (**Attachment 6**), signed by the unit commander to hand-carry classified materials. DD Form 2501 is an accountable form; SAs are responsible for ordering and maintaining this form.

2.2.4. Unit security assistants will have their facility Assistant contact 8 CES customer service for container lockouts/repairs and Preventive Maintenance Inspections (PMI) of their security containers/vaults/secure storage rooms. PMIs are required every five years for security containers, vaults, and secure storage rooms utilizing the Operational Visual Inspection (OVI) Checklist.

2.2.5. The signed annual Security Information Files (SAR) Review results is the unit Commander's approval on granting personnel access to classified information in Defense Information System for Security (DISS).

3. Personnel Security: The goal of the unit's personnel security program is to ensure personnel entrusted with classified or sensitive information are loyal, reliable, and trustworthy to protect and safeguard our nation's secrets.

3.1. Unit commanders are responsible for:

3.1.1. Conducting their annual SAR review in the months of July/August each year to determine the accuracy of position coding. **NOTE:** Due to the annual turnover period during the month of May/June for the 8 FW, the SAR review will be conducted in July/August to allow new commanders the opportunity to validate the accuracy of their Unit Manning Document (UMD).

3.2. Unit security assistants are responsible for:

3.2.1. Verifying a favorable Host Agency Check (HAC) has been completed on KFNs employed in their organization. HAC are conducted every three years by 8 SFS.

3.2.2. Verifying a current and favorable HAC has been completed on KFNs prior to submitting an AF Form 2586, *Unescorted Entry Authorization Certificate*, for badge issuances for PL 3 & 4 type resources. 8 SFS Pass and Registration Section maintains approved USFK Form 82E which are the "Host Nation" equivalent for KFNs employed at Kunsan AB.

3.2.3. Incorporating visitor access procedures and security measures into the unit's Operating Instruction (OI) for cleared/uncleared personnel requiring access to classified information or unit facilities containing classified information.

3.2.4. Submitting 8 FW Clearance Investigation Request Form (Annex I) to 8 FW/IP for initial and periodic reinvestigation security clearance request.

3.2.5. Submitting memorandum (Annex J) to the unit commander to appoint personnel as derivative classifiers.

4. Industrial Security: The goal of the unit's industrial security program is to ensure contractors are properly incorporated into the unit's security program and maintains compliance with DoDM 5220.22_AFMAN 16- 1406.

4.1. Unit security assistants are responsible for:

4.1.1. Performing as the sponsoring activity's point of contact for security matters pertaining to industrial security contracts within their organization.

4.1.2. Ensuring contractors are denied access to sensitive or classified information until the 8 FW/IP has received and verified all appropriate classified contract documentation, to include renewal contract documentation.

4.1.3. Issuing and retaining the In-Processing Checklist for Contractors Requiring a CAC ID (**Attachment 3**) on contractors sponsored by the unit.

4.1.4. Ensure contractors are incorporated into the unit's security training program.

5. Insider Threat: The purpose is to prevent, deter, detect and mitigate insider threats to national security and Air Force assets.

5.1. Commanders and Directors at the wing-level and below will:

5.1.1. Report any incident meeting one or more of the DoD Insider Threat Management and Analysis Center (DITMAC) threshold-level events to the 8 FW/IP office within 3 calendar days. The 8 FW/IP must report non-compliance to the 8 FW Deputy Commander (8 FW/CD).

PETER E. KASARSKIS, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDM 5200.01_AFMAN 16-1404 Vols 1-3, *Information Security Program*, 12 Apr 2022

DoDM 5200.02_DAFMAN 16-1405, *Air Force Personnel Security Program*, 29 Nov 2023

DoDM 5220.22_AFMAN 16-1406 Vol 2, *National Industrial Security Program*, 8 May 2020

AFI16-1402, *Counter-Insider Treat Program Management*, 17 Jun 2020

AFI33-322, *Records Management and Information Governance Program*, 28 Jul 2021

DAFI 31-101, *Integrated Defense (CUI)*, 11 Apr 2023

USFK Regulation 190-7, *Installation Access Control*, 6 Nov 2014

DoDI 5200.46, *DoD Investigative Adjudicative Guidance for Issuing the Common Access Card (CAC)*, 2 Nov 2020

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

DD Form 1144, *Support Agreement*

USFK Form 82-E, *Application for Installation Base Pass*

DD Form 2501, *Courier Authorization*

AF Form 2586, *Unescorted Entry Authorization Certificate*

SF 312, *Classified Information Nondisclosure Agreement*

DD Form 254, *Department of Defense Contract Security Classification Specification*

AF Form 2583, *Request for Personnel Security Action*

AF Form 2587, *Security Termination Statement*

USFK Form 37-EK, *Installation/Base Pass*

Abbreviations and Acronyms

AB—Air Base

ADCON—Administrative Control

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFRIMS—Air Force Records Information Management System

CAC—Common Access Card

CATO—KUNSAN—Contract Air Terminal Operations-Kunsan

CNWDI—Critical Nuclear Weapon Design Information

DoDM—Department of Defense Manual

DISS—Defense Information System for Security

DITMAC—DoD Insider Threat Management and Analysis Center

DRU—Direct Reporting Unit

DSN—Defense Switched Network

EMSEC—Emission Security

EO—Executive Order

FW—Fighter Wing

GSA—Government Services Agency

HAC—Host Agency Check

IAW—In Accordance With

ID—Identification

IP—Information Protection

ISA—Intra-Service Support Agreement

Intel—Intelligence

IT—Information Technology

KFNs—Korean Foreign Nationals

KRO—Korea Readiness Operation

LIPME—Location Information Protection Management Evaluations

MOA—Memorandum of Agreement

MAJCOM—Major Command

NATO—North Atlantic Treaty Organization

NBIS—National Background Investigation Services

NACI—National Agency Check with Inquiries

OI—Operating Instruction

OPR—Office of primary Responsibility

OSI—Office of Special Investigations

OVI—Operational Visual Inspection

PL—Protection Level

PMI—Preventive Maintenance Inspection

POC—Point of Contact

RDS—Records Disposition Schedule

SA—Security Assistant

SAR—Security Access Requirement

SIF—Security Information Files

TS—Top Secret

VGSA—Visitor Group Security Agreement

UMD—Unit Manning Document

UMPR—Unit Manning Personnel Roster

UNIT SA—Unit Security Assistant

US—United States

USFK—United States Forces Korea

USFKR—United States Forces Korea Regulation

8 FW/IP—8th Fighter Wing Information Protection Office

8 OSS—8th Operations Support Squadron

8 SFS—8th Security Forces Squadron

8 FW/CC—8th Fighter Wing Commander

8 FW/CD—8th Fighter Wing Deputy Commander

8 LRS—8th Logistics Readiness Squadron

8 CES—8th Civil Engineer Squadron

Attachment 2

INFORMATION PROTECTION WAIVE OUT MEMORANDUM

Figure A2.1. Information Protection Waive Out Memorandum.

APPROPRIATE LETTERHEAD

MEMORANDUM FOR 8 FW/IP DATE

FROM: (The organization that has ADCON of the unit requesting to be waived out)

SUBJECT: Request to Waive Out of Information, Personnel, and Industrial Security Programs

1. In accordance with Intra-Service Support Agreement (ISA) XX0000-00-0000, (list ADCON or parent organization who will provide oversight for the unit to be waived), provides security program oversight for (list unit to be waived), located at (list waived unit's location), Republic of Korea. (List ADCON/parent organization) will conduct annual program reviews as required by (list parent organization), Air Force, and DoD policies. Other security administrative requirements such as, unit security manger appointment letters, unit security operating instruction, semiannual self-inspection, initial and annual vault/open storage certifications, annual position code validations, annual classified cleanout, and SF Form 312, *Classified Information Nondisclosure Agreement*, will be processed through (list parent organization that has ADCON).

2. List waived organization. Will report and process all security violations as defined in DoDM 5200.01_AFMAN 16-1404 Vols 1-3, *Information Security Program*, to the (list ADCON/parent organization), Information Protection Office (IPO). (List ADCON/parent organization's IP) is responsible for accomplishing all actions associated with security violations and as listed in DoDM 5200.01_AFMAN 16-1404 Vols 1-3.

3. Please direct any questions you may have to my Point of Contact (POC), (Rank, First MI Last) at DSN XXX-XXX-XXXX.

Name of Parent Organization Commander who has ADCON, Colonel, USAF
Commander

Attachment 3

IN-PROCESSING CHECKLIST FOR CONTRACTORS REQUIRING A CAC ID

Figure A3.1. In-Processing Checklist for Contractors Requiring a CAC ID.

In-Processing Checklist for Contractors Requiring a CAC ID

Contractor's Name	Company's Name	Sponsoring Unit	DSN:

Welcome to Kunsan Air Base; home of the Wolf Pack! You are responsible for contacting all of the below offices (*in the sequential order*) within 15 calendar days of your contract start date. The first & last office (Sponsoring Unit Security Assistant) will keep your form upon completion. **IMPORTANT**: This checklist covers **mandatory** agencies you are required to in-process. You may need to in-process other agencies (post office, immigrations office, etc) which are not part of this checklist.

ITEM	Unit Security Assistant	Date	Initial	Comments
1	Security In-processing (JPAS, Security Briefing, etc)			
2	Vetting of Background Check or Security Clearance			

As the Unit Security Assistant, I have validated member's existing background check/security clearance and have annotated the information below. If member doesn't have a favorable background check or a current security clearance, one will be initiated.

	Clearance Level:	Type of Investigation (Circle): HAC by 8 SFS or NACI (T1) NACLC, ANACI, PRS (T3), SSBI SBPR (T5)
	Clearance Grant Date:	Date Investigation Completed:
	Unit Security Assistant (Printed Name):	Unit Security Assistant Signature:

ITEM	8th Fighter Wing/Information Protection Office Location: Bldg 1305, Rm 223. DSN: 782-1585	Date	Initial	Comments
1.	Copy of Contract/Statement of Work			
2.	Vetting of Background Check & Security Clearance			
3.	Determine if SIPRNet is listed on SOW or DDFM 254			

ITEM	8th Force Support Squadron/Manpower Office Trusted Associate Sponsorship System (TASS) Location: 8 FSS, Bldg 755, Rm 321 DSN: 782-4020	Date	Initial	Comments
1	Vetting of Identification (Employee MUST have two forms of ID)			
2	Provide a copy of front page of Employee's Contract (needs to have contract number and expiration of date)			
3	TASS Coordinator will give employee DD Form 2842 for ID Card			

ITEM	8th Force Support Squadron/Customer Service Desk Location: Bldg 755, Rm 119 DSN: 782-7073	Date	Initial	Comments
1	Verification of DEERS Enrollment			
2	Issuance of CAC/ID Card			

ITEM	8th Security Forces Squadron/Pass & ID Section Location: Bldg 1310 DSN: 782-4000/4744	Date	Initial	Comments
1	Registration into DBIDS (required for Base Access)			
2	Ration Control Card			
3	Driver's License for Privately Owned Vehicle			
4	Vehicle Registration			
5	Restricted Area Badge (if required)			Requires a favorable T-1 or HAC or higher before issuance

ITEM	Unit Cyber Security Liaison (CSL) DSN 782-2666	Date	Initial	Comment
1	NIPRNet Access (Requires DD 2875, NIPR USB Memorandum, AF Form 4394, and must be in Contract)			Requires a favorable T1 or HAC or higher to be granted NIPRNet access

ITEM	Unit Cyber Security Liaison (CSL) DSN 782-2666	Date	Initial	Comments
1	SIPRNet Access (Requires DD 2875, AF Form 4394, DD Form 2842, and must be in Contract) **NOTE**: If N/A, the IP Office will sign off this section			Requires a T3 or higher to be granted SIPRNet access

ITEM	Unit Security Assistant	Date	Initial	Comments
1	Verify Checklist Completion			
2	Turn in checklist to Unit Security Assistant			
NOTE:	HAC = Host Agency Check		Last Rev:	8 Sep 2019

Attachment 4

SECURITY ASSISTANT APPOINTMENT MEMORANDUM TEMPLATE

Figure A4.1. Security Assistant Appointment Memorandum Template.

APPROPRIATE LETTERHEAD

Date

MEMORANDUM FOR 8 FW/IP

FROM: ORG/CC

SUBJECT: Unit Security Assistant Appointment Letter

1. The following personnel have been appointed as Security Assistants for the Unit/Squadron:

PRIMARY	**ALTERNATE**
RANK LAST NAME, FIRST MI	RANK LAST NAME, FIRST MI
DSN: 782-xxxx	DSN: 782-xxxx
Firstname.lastname@us.af.mil	Firstname.lastname@us.af.mil
DEROS: Month 20xx	DEROS: Month 20xx

2. In association with their duties as security assistants, the above listed personnel are authorized/delegated the following:

a. Access/Management of the Defense Information System for Security (DISS) and National Background Investigation Services (NBIS) programs.
b. To appoint custodiams for classified containers, open storage rooms, and vaults.
c. Access to unit's UMD/Unit Manning Personnel Roster (UMPR) rosters to validate clearance access levels.
d. Authorized to pick up derogatory information files from the 8 FW/IP office.
e. Issue DD Form 2501/Courier Authorization to authorized unit personnel for transportation of classified information/equipment.
f. Coordinating/approving official for the unit and authorized to sign the annotated section of AF Form 2586.

3. This letter supersedes any previous appointment letter.

Commander's Signature Block

Attachment 5

EMERGENCY PROTECTION, REMOVAL, AND DESTRUCTION PLAN

A5.1. General. This plan establishes procedures for the emergency protection, removal, and destruction of classified material. Use this plan to develop unit implementing instructions. Consider the following:

A5.1.1. Threat**.** Two threats, which affect the security of classified material on Kunsan AB, are natural disasters and the threat of attack by hostile elements. Typhoons and the ever-present threat of fire are considered natural disasters. Intelligence information concerning civil disturbances, terrorist acts, and enemy action will be made available to allow time for an orderly and systematic destruction of classified holdings. The greatest threat to classified information in these circumstances is capture by the enemy.

A5.1.2. Limiting Factors. Insufficient incinerators to destroy all classified material when immediate destruction is necessary coupled with non-availability of personnel during emergency conditions.

A5.2. Execution. The wing commander normally implements this plan through installation senior staff directives. The senior individual in an assigned area containing classified material may implement the plan when circumstances warrant.

A5.2.1. **Phase One.** Emergency Protection Procedures are initiated for natural disasters, acts of terrorism, bomb threats, or minor civil disturbances. These events generally occur without warning, so the senior individual may initiate execution. When safety or security is not threatened, return classified material to an approved security container.

A5.2.1.1. Natural Disasters. After evacuation, notify security forces and fire department of insecure classified material and its location. When severe weather is not a factor, custodians will post personnel around affected facilities, to prevent the unauthorized removal of classified material. After the area is declared safe, entry into the facility will be limited to classified custodians, security forces, and fire department personnel tasked to recover classified material.

A5.2.1.2. Bomb Threats. When notified of a bomb threat, evacuate and leave everything untouched to preserve evidence. After evacuation of the facility, make every effort to visually monitor entry into the affected area. Office personnel will notify their Unit SA, Security Forces, or Fire Department personnel that classified material was left insecure, its location, and any other pertinent related information. Inventory classified holdings upon termination of the threat, and immediately report discrepancies to your security Assistant or supervisor.

A5.2.1.3. Minor Civil Disturbances. Minor civil disturbances such as student uprisings or protests are always a possibility in the area of Gunsan city. In the event these activities are brought to the installation, classified material should be returned to its security container. If the situation warrants, office assistants might consider moving classified holdings to a more secure area. Facilities with open storage areas will man their facilities on a 24-hour basis until the threat passes. Arming personnel to protect classified material is not necessary. Prepare to implement Phase Two of this plan if the situation worsens.

A5.2.2. **Phase Two.** Emergency Removal and Evacuation Procedures. This phase is initiated upon serious incidents of civil unrest or threat of enemy action. A time-phased reduction of classified holdings begins during this stage.

A5.2.2.1. All classified material will be separated from unclassified holdings. Office assistants will make a determination as to what classified must remain on Kunsan AB for mission accomplishment. Classified holdings, which must be maintained for operational or historical significance, will be evacuated to a more secure environment, if deemed necessary by the 8th Fighter Wing Commander (8 FW/CC) or higher authority.

A5.2.2.2. If the order to evacuate classified holdings is given and if time allows, office assistants will place materials not necessary for mission accomplishment into field safes (260 lbs. or less) or cardboard boxes. Separate those holdings by destruction priority and mark that priority on the outside of the box. A list of the contents of each box will be compiled. Place one copy of the list inside a clearly marked envelope, and tape it to the inner lip of the box. Retain a copy of the list, remembering to mark it with the appropriate level of classification, if applicable. Seal all boxes with tape to prevent accidental opening while in transit. The UNIT SA will coordinate the pickup of classified set aside by offices assigned to the account, and ensure they are transported to building 2860, Contract Air Terminal Operations Kunsan (CATO KUNSAN), in a timely manner.

A5.2.2.3. If the situation continues to deteriorate, prepare to implement Phase Three.

A5.2.3. **Phase Three.** Emergency Destruction Procedures. This phase will be executed when an immediate threat exists, such as the installation being overrun or lost to an attacking force. Under these conditions, destruction of classified should begin early to preclude its loss. Premature destruction is considered inconsequential when measured against the possibility of loss or compromise of information or equipment. In the event the wing commander or higher authority cannot disseminate the order, the senior individual present in the office or unit will initiate this phase. The senior-ranking individual must make a commonsense determination that a threat exists in which material could be lost or compromised if emergency destruction is not initiated.

A5.2.3.1. UNIT SAs and security container custodians will reduce the number of classified holdings to the absolute minimum required for mission accomplishment. Unit Operating Instructions will identify the destruction equipment they will use if time permits. Ensure material is destroyed in order of priority. Units will mark containers to be destroyed with organization and office symbol.

A5.2.3.2. UNIT SAs will identify a metal drum or container (such as a metal trash can), to be used for the purpose of emergency destruction, at each facility storing classified material. Incendiary devices or flammable liquids may be used to speed destruction. A list of all materials destroyed will be accomplished. Burning classified material will be used as an emergency method only and is not approved for routine destruction.

A5.3. Task Organizations.

A5.3.1. 8 LRS will provide personnel to train other unit personnel on cargo preparation and pallet building so units can palletize classified material during implementation of Phase Two.

A5.3.2. CATO KUNSAN will provide personnel to load the aircraft after palletizing.

A5.3.3. 8 OSS/Intel will maintain the 8 FW's capability to bulk shred classified information for contingency/emergency operations.

A5.3.4. Each commander/staff agency chief will:

A5.3.4.1. Assign priorities to classified material for emergency destruction purposes. Priority I - Top Secret and all Critical Nuclear Weapon Design Information (CNWDI); Priority II – Secret; Priority III – Confidential.

A5.3.4.2. Provide one person to palletize. This person will report to 8th Logistics Readiness Squadron (8 LRS) to assist inspecting palletized classified material to ensure it meets airworthiness standards and has the proper documentation.

A5.3.4.3. Designate government vehicles to transport classified materials. Contact 8 LRS when no unit vehicles are available.

A5.3.4.4. Develop secondary destruction procedures. Label shredders with Authorized Shredder for Classified Destruction provided by the Information Security Program Assistant.

A5.3.4.5. Formulate unit operating instructions and checklists tailored to compliment this attachment. These instructions will be placed near security containers.

A5.3.4.6. Ensure all assigned personnel are familiar with these procedures. UNIT SAs should exercise this plan annually.

A5.4. Logistics and Administration. It is imperative units establish provisions for local destruction of Priority II & III material. Routine destruction of classified holdings is the key to efficient emergency destruction.

A5.5. Command Authority. The 8 FW/CC will exercise command authority for the Emergency Protection, Removal, and Destruction of classified material on Kunsan AB

Attachment 6

DESIGNATED CLASSIFIED COURIER TEMPLATE

Figure A6.1. Designated Classified Courier Template.

APPROPRIATE LETTERHEAD

Date

MEMORANDUM FOR 8 FW/IP

FROM: ORG/CC

SUBJECT: Designated Classified Couriers for (Unit)

References: (a) DoDM5200.01V3_AFMAN16-1404V3, *Information Security Program: Protection of Classified Information*

1. The following individuals have been selected/designated as official couriers for the United States Government. Upon request they will present their official identification card DD Form 2AF, DODID # and courier authorization card DD Form 2501, Serial Number (SN) (Top right of card).

	Rank/Name	**Last 4 of SSN**	**Eligibility Level**	**DEROS (Month Year)**
*				

2. All personnel have been briefed by the unit security assistant on their responsibilities in safeguarding classified during transportation. Personnel with (*) are also authorized to transport classified internationally.

3. The individuals listed above are authorized to hand-carry sealed packages between this organization on Kunsan AB, RoK and the listed locations, traveling by air and car. Packages are identified on the outside by the marking "**OFFICIAL BUSINESS – MATERIAL EXEMPTED FROM EXAMINATION**" bearing the signature of the undersigned.

4. A copy of this letter will be maintained in the unit security assistant. The letter supersedes any previous letter.

Commander's Signature Block

Attachment 7

SECURITY ASSISTANT CONTINUITY BINDER

A7.1. Section 1, Information Security.

A7.1.1. **Tab A – Appointment Letters & Training Certificates**

A7.1.2. **Tab B – Unit Security Assistant Training Slides**

A7.1.3. **Tab C – Clear and Un-Clear Personnel Training Log**

A7.1.4. **Tab D – Unit Security Operating Instructions**

A7.1.5. **Tab E – Open Storage Room/Vault Request** (Initial request/justification letter, structural and alarm survey from 8th Civil Engineer Squadron (8 CES), and physical security survey from 8 SFS)

A7.1.6. **Tab F – Approval Memorandums for Open Storage Room/Vault**

A7.1.7. **Tab G – Government Services Agency (GSA) Safes, Printers and Shredders Location List**

A7.1.8. **Tab H– Unclassified Inventory List of Safe/Room/Vault Contents**

A7.1.9. **Tab I – Quarterly Security Assistant Meeting Minutes** (Last four copies)

A7.1.10. **Tab J – Miscellaneous**

A7.2. Section 2, Personnel Security.

A7.2.1. **Tab A – Clearance Investigation Request Form**

A7.2.2. **Tab B – Copy of UMD and Unit Manning Personnel Roster (UMPR)**

A7.2.3. **Tab C – Current Periodic Reinvestigation Report** (within the last 45 days)

A7.2.4. **Tab D – Annual SAR and/or Top Secret (TS) Revalidation Review** (Last 2 years)

A7.2.5. **Tab E – AF Form 2583, *Request for Personnel Security Action*, for Interim Security Clearance and Access to Classified** (Retain the AF Form 2583 until the member PCS)

A7.2.6. **Tab F – AF Form 2587, *Security Termination Statement*** (Retain for two years)

A7.3. Section 3, Industrial Security.

A7.3.1. **Tab A – Industrial Security Folder** (Includes DD Form 254, *Department of Defense Contract Security Classification Specification*, Visit Group Security Agreement (VGSA), On-site Security POC, 8 FW annual self- assessment report and DISS Visit Request)

Attachment 8

CLASSIFIED ACCESS AUTHORIZATION EXAMPLE

Figure A8.1. Classified Access Authorization Example.

REQUEST FOR PERSONNEL SECURITY ACTION

AUTHORITY: 10 U.S.C. 8012; 44 U.S.C. 3101; and EO 9397.
PRINCIPAL PURPOSES: To identify investigation, security clearance, unescorted entry requirements, and special access program authorizations.
ROUTINE USES: To request personnel security investigations, record emergency or limited access authorization, entry to restricted areas, and to record special access program authorizations. SSN is used for positive identification of the individual and records.
DISCLOSURE IS VOLUNTARY: Failure to information and SSN could result in assignment to less sensitive duties.

I. IDENTIFYING INFORMATION

1. NAME (Last, First, Middle, Maiden)	2. ORGANIZATION OR FIRM SPONSOR
Doe, John P.	8 FWIOZ

3. GRADE	4. SSN	5. CITIZENSHIP
A1C	Last 4 Only	☑ US CITIZEN ☐ IMMIGRANT ALIEN ☐ NON-US NATIONAL

6. DATE OF BIRTH	7. PLACE OF BIRTH (City, State and Country)
N/A	N/A

II. INVESTIGATION, CLEARANCE, ELIGIBILITY, ENTRY AND ACCESS REQUIREMENTS

8. INVESTIGATION REQUIREMENT	9. CLEARANCE, ENTRY OR ACCESS REQUIREMENT	
	☐ ONE-TIME ACCESS	☐ LIMITED ACCESS
☐ National Agency Check and Inquiries (NAC)	☐ INTERIM CLEARANCE	☐ SPECIAL ACCESS
☐ National Agency Check with Law and Credit (NACLC) or Access National Agency Check and Inquiries		☐ UNESCORTED ENTRY
☐ Single Scope Background Investigation (SSBI)	☐ TOP SECRET	☐ Priority Level 1
☐ Secret Periodic Reinvestigation	☑ SECRET	☐ Priority Level 2
☐ SSBI or PPR Periodic Reinvestigation		☐ Priority Level 3
		☐ Priority Level 4

III. LOCAL FILES CHECK

10. TO	11. FROM
8 XXX/Commander	8 XXX/Unit Security Manager

12. DATE	13. TYPED NAME, GRADE AND TITLE OF REQUESTER	14. SIGNATURE
12/25/2015	Smith, Jane M., SSgt, Unit Security Manager	Click to sign

IV. MEDICAL RECORDS CHECK

15. I CERTIFY a medical records check required by AFI 31-501 or its replacement has been completed and no information exists, unless shown in Section VII, which would preclude the granting of eligibility of security clearance, access to special programs or unescorted entry to restricted areas.

16. DATE	17. TYPED NAME AND GRADE OF BASE DIRECTOR, MEDICAL SERVICES	18. SIGNATURE
N/A	N/A	Click to sign

V. SECURITY POLICE RECORDS CHECK

19. I CERTIFY a security police records check required by AFR 205-32, has been completed and no information exists, unless shown in Section VII, which would preclude the granting of a security clearance, unescorted entry to restricted areas, or access to special program classified information.

20. DATE	21. TYPED NAME AND GRADE OF SECURITY POLICE OFFICIAL	22. SIGNATURE
N/A	N/A	Click to sign

VI. ACCESS AUTHORIZATION

☐ ONE-TIME ACCESS	☐ LIMITED ACCESS	☐ CNWDI	☐ NATO	☐ RD	NC2-ESI
				☐ CONTINUING	☐ ONE-TIME

23. I CERTIFY the named individual requires access to the above special program(s), meets all investigative and clearance requirements and has been briefed security on program responsibilities as outlined in the governing directive. If applicable, emergency or limited access is necessary and will not endanger the national

24. DATE	25. TYPED NAME, GRADE AND TITLE OF APPROVING AUTHORITY	26. SIGNATURE
Date	Commander Name	Click to sign
27. DATE	28. TYPED NAME, GRADE AND TITLE OF SPECIAL ACCESS PROGRAM CERTIFYING OFFICIAL	29. SIGNATURE
		Click to sign

VII. REMARKS

30. *(If more space is needed, use reverse and show item number being continued)*

Last Invest. date 20150101. CC Appt Derivative Classifier. Auth SIPRNet/CENTRIX-K Trng Certs: Marking 00/00/15, Derivative 00/00/15

AF IMT 2583, 20140404, V3 PREVIOUS EDITION WILL BE USED. PRIVACY ACT INFORMATION: The information in this form is FOR OFFICIAL USE ONLY. Protect IAW the Privacy Act of 1974.

Attachment 9

SECURITY ASSISTANT APPOINTMENT MEMORANDUM TEMPLATE

Figure A9.1. Security Assistant Appointment Memorandum Template.

APPROPRIATE LETTERHEAD

Date

MEMORANDUM FOR RECORD

FROM: ORG/CC

SUBJECT: DERIVATIVE CLASSIFIERS for ORG

1. The following personnel have been identified as derivative classifiers and are charged to ensure appropriate standards are met when creating derivative classified documents in accordance with Executive Order (EO) 13526 and DoDM 5200.01_AFMAN 16-1404:

	Rank/Name	Last 4 of SSN	Eligibility Level	DEROS (Month Year)
*				

2. In association with their duties as derivative classifier, derivative classifiers are authorized/delegated the following:

a. Ensure the proper classification markings are applied when creating derivative classified document in accordance with local directives and DoDM 5200.01_AFMAN 16-1404.
b. Complete and maintain Derivative Classifier training annually in accordance with EO 13526 and USDi Memorandum dated 31 Jan 2019.

3. All derivative classifiers were briefing on my expectation and their duties/responsibilities as derivative classifiers. The letter supersedes any previous appointment letter.

4. Questions regarding this program should be directed to **Rank First Last Name**/Unit Security Assistant. He/She can be reached at first.lastname@us.af.mil or DSN (315)782-xxxx.

Commander's Signature Block