BY ORDER OF THE COMMANDER
GOODFELLOW AIR FORCE BASE

GOODFELLOW AIR FORCE BASE
Supplement

22 NOVEMBER 2019
Certified Current on, 25 February 2020
Operations Support

INFORMATION SECURITY PROGRAM MANAGEMENT

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: 17 TRW/IP

Certified by: 17 TRW/CV
(Col Robert G. Ramirez)

Supersedes: AFI16-1404_GOODFELLOWAFBSUP, 23 January 2017

Pages: 14

This supplement implements and extends the guidance of DoDM 5200.01, DoD Information Security Program Volumes 1-4, 24 February 2012, and Air Force Guidance Memorandum, AFI 16-1404 *Air Force Information Security Program*, 14 September 2018. This publication may be supplemented at any level, but all direct supplements must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination prior to certification and approval. This supplement applies to all assigned military and civilian personnel, contract personnel, and tenant personnel as required. This supplement also applies to Air Force Reserve Command (AFRC) and to Air National Guard (ANG) units gained by Goodfellow upon mobilization and when published in the ANG Master Catalogue. Ensure all records created as a result of processes prescribed in this publication are maintained according to AFMAN 33-363, *Management of Records*, and disposed of according to 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 OPR using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate functional's chain of command.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. Major changes include self-inspections, time USAs have to complete training, and STC requirement.

2.4.4.1. The last business day in January will be focused on disposing of unneeded classified material (clean-out-day). Each office that maintains classified material will establish an MFR stating the material was reviewed and unneeded material was destroyed IAW AFI 16-1404 **para 2.4.4**.

2.5. The Information Security Program is established on Goodfellow AFB (GAFB) with the 17th Training Wing Information Protection Office (17 TRW/IP) as the office of primary responsibility (OPR) and is the point of contact for all matters pertaining to information security on GAFB.

2.5.3.1. Security Assistant meetings will be held as needed, but not less than annually. Each unit will send a representative to ensure information is passed down. GSUs will be provided dial-in conference information prior to the meeting for virtual attendance.

2.5.4. **(ADDED)** Conduct an annual Information Protection Management Evaluation (IPME) on each unit having access to classified information and a biannual IPME on those units that do not have access to classified information. Report will be uploaded into the Enterprise Protection Risk Management (EPRM) tool. Commanders will coordinate on the corrective actions report.

2.5.5.1.4. Security containers with both Communications Security (COMSEC) material and collateral material, will coordinate with COMSEC and 17 TRW/IP offices. Establish a single set of emergency procedures for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. These procedures will be coordinated through the security assistant, 17 TRW/IP, 17 CES/CEF, and 17 CS/SCXS COMSEC account managers.

2.5.5.3. For transient personnel in the possession of Sensitive Compartmented Information (SCI), the 17 TRG/SSO provides temporary storage. The 17 TRW Command Post (17 TRW/CP) provides temporary storage for all other classified material. The following applies to classified material temporarily stored by the 17 TRW/CP. Couriers of classified material will be directed to the Emergency Control Center (ECC). The Security Forces Controller will verify the courier's credentials, notify the command post controller, and escort the courier to the command post where the material will be stored.

2.7.1.3. Commanders will designate, in writing, an activity security assistant, IAW DoD 5200.01-V1 Enclosure 3. Appoint an individual for a minimum of 12 months. They will be given the necessary authority to ensure personnel adhere to program requirements. Provide the designated activity security assistant direct access to activity leadership and ensure he or she is organizationally aligned to ensure prompt and appropriate attention to program requirements. Appointments will identify all offices or agencies included in their information security program. (See **Attachment 2** for format).

2.7.1.3.1. **(ADDED)** Commanders will ensure activity security assistants complete training CBTs within 3 months from appointment.

2.7.1.3.2. **(ADDED)** Commanders will ensure personnel in sensitive duties receive initial and refresher training on the national security implications of their duties and the individual's responsibility to meet the standards and criteria for security eligibility.

2.7.1.3.3. **(ADDED)** Expeditiously report behaviors that indicate impaired judgement, reliability, or trustworthiness to the DoD Central Adjudication Facility through the Security Assistant. See December 29, 2005 White House Memorandum, Intelligence Community Policy Guidance 704.2 or their successor documents, as appropriate for additional information.

2.7.1.3.4. **(ADDED)** When an action is questionable as to whether or not it should be reported to DOD CAF, err on the side of caution and report it or ask 17 TRW/IP for a determination.

2.7.4.2. The unit commander will identify in writing anyone who derivatively classifies information but does not have access to a classified information system, and provide a copy of the letter to 17 TRW/IP.

2.7.7. The commander will sign the unit security plan/instruction and will include procedures for protection of classified material cradle-to-grave.

2.7.7.2.1. Unit security plans/instructions will address precautions taken to prevent cellular/PCS, radio frequency (RF), infrared (IR) wireless devices, or other devices such as cell phones and tablets, and devices that have photographic or audio recording capabilities, AKA unauthorized equipment, from going into any collateral classified working area. The security plans/instructions will also cover procedures to be used when unauthorized equipment enters into an area where classified information is discussed or processed.

2.7.7.2.2. The commander, or documented designee over the area in which permission to use a fitness device is requested, is responsible to fully consider mission requirements and other systems/network enclaves collocated within the classified processing area. With the unit commander's authorization, PWFDs may be used in proximity of Air Force Enterprise accredited classified systems with no separation.

2.7.7.2.3. This PWFD policy only applies to collateral classified areas/computer systems. For fitness devices in Special Compartmented Information Facilities (SCIFs) contact 17 TRG/SSO for approval. For areas generating, storing or repairing COMSEC material contact the 17 CS/ IA office.

2.7.7.2.4. The commander will appoint a knowledgeable individual/office to complete any research required to determine if the device will be authorized. The person performing the research will be someone other than the requester.

2.7.7.2.5. The commander or designee responsible for the area identified will approve the use of the PWFD by endorsing the completed copy of the Authorization Request. See 17 TRW/IP for official memorandum. The MFR will be updated annually.

2.7.7.2.6. Once endorsed, a copy of the user request and authorization will be provided to 17 TRW/IP to obtain an authorization badge. The badge will be worn behind other badges, if applicable or prominently displayed above the waist, on the exterior of the outermost garment, easily viewable while in an area where authorization is required. The badge will be removed when no longer needed.

2.7.7.2.7. The unit is responsible for ensuring only approved PWFDs are brought into sensitive areas.

2.7.7.2.8. If an unauthorized PWFD enters into a classified processing area, it will be reported to 17 TRW/IP. After the device has been reviewed the incident will be determined to be a security infraction or a violation.

2.7.7.2.9. If a violation occurs the PWFD will be treated as classified and will be destroyed accordingly. The PWFD will be hand-receipted to 17 TRW/IP. After destruction has been completed, the hand-receipt will be signed and given to the security assistant to be maintained with the investigation records.

2.7.7.2.10. If at any time a PWFD is out of the owners control (ex: lost and found), the device will be considered potentially compromised and will not be authorized back into a secure facility. It is up to the integrity of the owner to notify the security assistant.

2.7.7.4. Identify procedures used to determine personnel security clearances, access, and need-to-know for visitors requesting access to classified material/areas.

2.7.7.5. **(ADDED)** Provide guidance to perform and annotate an operational check of unit owned shredders to ensure destruction equipment is performing as required. (Not missing teeth, shred size meets the 1 mm x 5 mm requirement, etc.).

2.7.13.1.1. If the agency security assistant does not perform this duty, the commander will appoint an official, in writing, to ensure security requirements are met.

2.7.13.1.2. AFI 16-1404 **Attachment 4** will be completed for each classified meeting/conference. The completed checklist will be turned-in/kept by the security assistant as proof of completion IAW records management requirements.

2.7.16. Appoint, in writing, at least one security container custodian for each security container maintaining collateral classified material. The SM will forward the signed letter to 17 TRW/IP.

2.8.7. Each security container will have procedures for the protection, removal, or destruction of classified material near the security container for easy access. Review the emergency procedures at least annually. Personnel who normally work in the same area as a security container should have a working knowledge of emergency procedures.

2.8.8. Authorized open storage areas will also post procedures for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. The procedures will be posted near the exit door of the area. Personnel working in the area will be familiar with how to use the emergency action cards.

2.8.9. Post the GOODFELLOWAFBVA 16-6 b, c, or d, unit/group security assistant designation, in a highly visible area in each unit. In units having multiple buildings consideration should be given to post the GOODFELLOWAFBVA 16-6 b, c, or d or ensure personnel in those areas are aware of who to contact in case of security issues.

2.8.10. **(ADDED)** The security assistant will notify 17 TRW/IP of planned and/or scheduled unit self-inspections in January each year to ensure annual inspections and unit self-inspections are conducted 6 months apart, as both inspections are required.

2.8.10.1. **(ADDED)** The security assistant will conduct the unit information, personnel, and industrial security self-inspection using the EPRM Checklist. Once complete, coordinate with 17 TRW/IP to upload the self-inspection info EPRM.

2.9. Security container custodians are responsible for the following.

2.9.1. Attend security container custodian training held by the 17 TRW/IP within 90 days of appointment.

2.9.2. Ensure an SF 701 and SF 702 are used to conduct end of day security checks for areas that process or store classified material. Use SF 702, Security Container Check Sheet, to show each and every security container/open storage area door opening and closing action. This check will be accomplished daily. Checks do not need to be accomplished on weekends and holidays unless the area is accessed. At the end of the normal duty day, accomplish an inspection of the container and document inspection on SF 702. When the container has not been opened, the end-of-day inspection will still be accomplished and documented by annotating in the opened by/closed by area "not opened," with the appropriate initials and time. Place the SF 702 near the security container or open storage area door. Prior to signing the SF 701, inspect the area for any classified material left outside of the secured container. Validate the SF 702 was signed off and attempt to open the security container to ensure the security container is locked. Security assistants will provide training for those personnel conducting end-of-day checks to include notification requirements. The SF 701 is not required for 24/7 work centers.

2.9.3. Maintain an accountability of all classified material placed in classified security containers/open storage areas.

2.9.4. **(ADDED)** Change lock combinations when required. Complete a new SF 700 and destroy the old one.

2.9.5. Coordinate with OPRs to ensure material is reviewed and destroyed as needed during the base annual "clean-out day". Certify, in an MFR, the clean-out was accomplished and identify for which security containers/open storage areas were included. Forward a copy to the security assistant. The security assistant will forward a copy to the 17 TRW/IP.

2.9.6. Coordinate with 17 TRW/IP to ensure only GSA certified locksmiths perform maintenance on security containers authorized to maintain classified material.

2.9.7. Use AFI 16-1404 Attachment 6 to perform an Operational Visual Inspection (OVI) on each security container and authorized open storage area every 5 years. Sign and date the inspection checklist. Keep a copy with the security container/authorized open storage area and give a copy to the agency security assistant.

5.2.4.4. Ensure all IT items in a mixed working environment are conspicuously marked with the highest classification the equipment is authorized to process to include unclassified markings. All items in a security container or secure room will be marked, to include unclassified markings on the top, bottom, front, back of each page, and on the spines of binders.

5.2.4.4.1. The GOODFELLOWAFBVA 16-1 will be posted on the exterior of a locked door when classified material is being processed for the protection of classified material.

5.2.4.4.2. The GOODFELLOWAFBVA 16-2 will be filled in and posted above machines authorized for the reproduction of classified material.

5.2.4.4.3. The GOODFELLOWAFBVA 16-3 will only be used in mixed environments above machines not authorized for the reproduction of classified material.

5.2.4.4.4. The GOODFELLOWAFBVA 16-4 will only be used on shredders that are authorized for the destruction of classified material in a mixed environment. The appropriate SF 700 series sticker will also be used to identify the level of classified authorized to be destroyed.

5.2.4.4.5. In areas where classified information is processed, ensure unclassified shredders are labeled with the GOODFELLOWFBVA 16-5 to inform individuals the equipment is not authorized for destruction of classified material.

5.2.4.5. In an environment where both classified and unclassified information is processed or stored, IT equipment will be identified according to highest level of classification contained in, contained on, or destroyed by that item. The SF 710, "Unclassified (Label)" shall be used to identify unclassified media or equipment. Place the label conspicuously to indicate the highest classification of material authorized for processing. The SF 710 is not required in areas where classified information is not processed or stored.

5.2.4.6. Storing Classified Material with Communications Security (COMSEC) Material. COMSEC material will be maintained according to COMSEC publications. COMSEC and collateral material may be maintained in the same security container but not in the same drawer. COMSEC will not be maintained in the locking drawer. COMSEC material is to be viewed only by those individuals with COMSEC access. Personnel without COMSEC access will not have the combination to the security container. An inventory is required for the non-COMSEC material. 17 TRW/IP personnel are not authorized to inspect COMSEC material. COMSEC manager is not authorized to inspect collateral material. All personnel with access to the security container will be familiar with access, maintenance, and inspection practices.

5.2.5.1. To prevent unauthorized disclosure of information on a hard drive or removable media before turn in refer to AFSSI 5020, Communications and Information Remanence Security, for procedures in clearing, sanitizing media, and approved methods and tools available.

5.2.5.2. The 17 TRG/CC and 17 TRG/SSO are responsible for the operations and control of the GAFB Central Destruction Facility. GAFBI 14-301, Personnel and Facility Sensitive Compartmented Information, outlines these responsibilities and procedures.

5.2.5.3. A copy of the approved Evaluated Products List highlighting the approved shredder will be taped on the inside of the authorized shredder door for inspection purposes.

5.2.6. **(ADDED)** Classified working areas must be kept as clean and clutter free as possible. The working environment must lend itself to working on classified or unclassified material without co-mingling the two by accident. A cluttered environment is considered a practice dangerous to security (PDS).

5.2.7. **(ADDED)** When planning for new open storage rooms/areas, ensure the area meets the Sound Transmission Class STC-50 or better.

5.3.2.1. Commanders and Directors will establish procedures to ensure hand-carrying collateral classified material is minimized to the greatest extent possible and does not pose an unacceptable risk to the information. Classified material can be hand-carried off base as a last resort if it is an immediate operational necessity/contractual requirement and the material cannot be sent via secure e-mail, secure facsimile transmission, official registered mail, and authorized Express mail. If the need arises, the security assistant and 17 TRW/IP will be notified immediately to assist with details.

5.3.2.2. Security Forces personnel conducting entry point checks will ensure any classified material carried by personnel departing the installation is accompanied by DD Form 2501,

Courier Authorization, or a courier authorization memorandum. Classified information must also be properly packaged (see DoDM 5200.01 V3 Enclosure 4 Paragraph 9).

6.1.1. Training will incorporate official CBTs whenever possible.

6.1.1.1. **(ADDED)** Training will be conducted following the Goodfellow Annual Training Plan as established by 17 TRW/IP. Coordinate with 17 TRW/IP for suggested modifications or changes.

7.3.1.1.1. The 17 TRW/IP is responsible for incidents involving all collateral material outside SCIFs. The 17 TRG/SSO is responsible for incidents involving all SCI material and collateral material under the control of the SCIF, unless otherwise determined by the 17 TRG/SSO.

7.3.1.1.2. 17 TRW/IP will brief the preliminary inquiry official on duties and responsibilities prior to the initiation of the investigation. Notify the 17 TRG/SSO immediately if a security incident involves sensitive compartmented information (SCI) material. 17 TRG/SSO requires notification anytime an individual, read into SCI, is involved in a security incident regardless of classification of information involved.

7.3.1.2.1. If the security incident cannot be completed within 10 duty days a 10-duty day extension letter will be signed by the unit commander. If more than 20 duty days are required to complete the investigation a 10-duty day extension letter will be signed by the group commander.

ANDRES R. NAZARIO, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING DOCUMENTS

References

AFSSI 5020, *Communications and Information Remanence Security*, 17 April 17, 2003

DoDD 5210.50, *Management of Serious Security Incidents Involving Classified Information*, October 27, 2014

DoDD 5205.07, "*Special Access Program (SAP) Policy*," July 1, 2010

DoDD 5230.09, *Clearance of DoD Information for Public Release*, August 2, 2008, Certified Current through August 22, 2015

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, April 14, 2004, Certified current as of April 23, 2007

DoDI 3305.13, *DoD Security Education, Training, and Certification*, February 13, 2014

DoDI 5010.40, *Managers Internal Control Program Procedures*, January 4, 2006

DoD 5200.08, *Physical Security Program*, April 9, 2007 Incorporating Change 1, May 27, 2009

DoDI 5210.02, *Access and Dissemination of RD and FRD*, June 3, 2011

DoDI 5210.83, *DoD Unclassified Controlled Nuclear Information (UCNI)*, July 12, 2012

DoD 3305.13-M, *DoD Security Accreditation and Certification*, March 14, 2011

DoDM 5200.01, Volume 1, *DoD Information Security Program*: *Overview, Classification, and Declassification*, February 24, 2012

DoDM 5200.01, Volume 2, *DoD Information Security Program*: *Marking of Classified Information*, 24 February 2012, Incorporating Change 2, March 19, 2013

DoDM 5200.01, Volume 3, *DoD Information Security Program*: *Protection of Classified Information*, 24 February 2012, Incorporating Change 2, March 19, 2013

DoDM 5200.01, Volume 4, *DoD Information Security Program*: *Controlled Unclassified Information (CUI)*, February 24, 2012

DoDM 5200.45, *Instructions for Developing Security Classification Guides*, April 2, 2013

DoDM 5205.07, Volume 4, *Special Access Program (SAP) Security Manual: Marking*, October 10, 2013

AFI 31-101, *Integrated Defense*, October 9, 2009, Incorporating Through Change 2, March 7, 2013

AFMAN 16-1405, *Air Force Personnel Security Program*, 1 August 2018

AFI 16-1404, *Air Force Information Security Program*, May 29, 2015

AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, February 18, 2014

AFI 33-115, *Air Force Information Technology (IT) Service Management*, September 16, 2014

AFI 90-201, *The Air Force Inspection System*, August 2, 2013

AFI 90-301, *Inspector General Complaints Resolution*, August 23, 2011

AFMAN 33-282, *Computer Security (COMPUSEC)*, March 28, 2012, Incorporating Change 1, January 15, 2015

AFMAN 33-360, *Publications and Forms Management*: *Communications and Information*, September 25, 2013

AFPD 16-14, *Security Enterprise Governance*, July 24, 2014

GAFBI 14-301, *Personnel and Facility Sensitive Compartmented Information*, Nov 22, 2016

TO 2012-076-014, *Classified Message Incident (CMI) Declaration Authority & Handling Procedures*, May 2012

Prescribed Forms

GOODFELLOWAFBVA 16-1, Attention Classified Work in Progress, Nov 2, 2016

GOODFELLOWAFBVA 16-2, Caution Authorized for Reproduction of Classified Material, Nov 10 2016

GOODFELLOWAFBVA 16-3, Stop Classified Reproduction is not Authorized on this Machine Stop, Nov 10, 2016

GOODFELLOWAFBVA 16-4, Authorized for Destruction of Classified Information, Nov 10, 2016

GOODFELLOWAFBVA 16-5, Authorized for Destruction of Unclassified Information Only, Nov 8, 2016

GOODFELLOWAFBVA 16-6b, Unit Security Assistant (Primary/Alternate), Sep 25, 2019

GOODFELLOWAFBVA 16-6c, Unit Security Assistant (Primary/Alternate/Alternate), Sep 25, 2019

GOODFELLOWAFBVA 16-6d, Unit Security Assistant (Primary/Alternate/Alternate/ Alternate), Sep 25, 2019

Adopted Forms

AF Form 3227, Privacy Act Cover Sheet, November 1, 1984

AF Form 1168, Statement of Suspect/Witness/Complaint, April 1, 1998

AF Form 1297, Temporary Issue Receipt, July 1, 1987

AFI 16-1404 Attachment 4, Classified Meeting/Briefing/Conference Checklist, May 29, 2015

DD Form 2056, Telephone Monitoring Notification Decal, May 2000

DD Form 2501, Courier Authorization, March 1988

Optional Form 89, Maintenance Record for Security Containers/Vault Doors, September 1989

SF 312, Classified Information Nondisclosure Agreement, July, 2013

SF 700, Security Container, April 2001

SF 701, Activity Security Checklist, November 2010

SF 702, Security Container Check Sheet, November 2010

SF 704, Secret Coversheet, August 1985

SF 705, Confidential Coversheet, August 1985

SF 707, Secret ADP Media Classification Label, January 1987

SF 710, Unclassified Label for ADP Media in SCI Facilities, January 1987

SF 711, Data Descriptor, January 1987

Attachment 2

SAMPLE SECURITY MANAGER APPOINTMENT MEMORANDUM

(USE GOODFELLOW AFB LETTERHEAD STATIONARY)

DATE

MEMORANDUM FOR 17 TRW/IP
17 TRG/SSO

FROM: Agency/Office Symbol

SUBJECT: Appointment of (Agency) Security Assistant

1. The individuals listed below are appointed as the (Unit) Security Assistants.

Primary – Rank, First/Last Name, Office Symbol, Phone Number

Signature _____

Assistant – Rank, First/Last Name, Office Symbol, Phone Number

Signature _____

Assistant – Rank, First/Last Name, Office Symbol, Phone Number

Signature _____

2. The security assistant will fulfill the following duties:

a. Manage and implement the information security program on behalf of the unit/CC, to whom he or she will have direct access.

b. Serve as the principal advisor and representative to the unit/CC in all matters pertaining to DoDM 5200.01 and maintain cognizance of all activity information, personnel, information systems, physical security functions to ensure that the information security program is coordinated in its execution and inclusive of all requirements in the DoDM 5200.01, as supplemented.

c. Provide guidance, direction, coordination, and oversight to designated assistant security assistants, security container custodians, and as appropriate, others in security management roles as necessary to ensure that all elements of the information security program are being administered effectively, efficiently, and in a coordinated manner.

d. Develop a written activity security instruction that shall include provisions for security container guarding classified information during emergency situations and military operations, if appropriate.

e. Ensure that personnel in the activity who perform security duties are kept abreast of changes in policies and procedures, and provide assistance in problem solving.

f. Formulate, coordinate, and conduct the activity security education and training program. Organizations with elements that are deployable for contingency operations shall ensure information security training, to include appropriate application to information systems, is an integral part of pre-deployment training and preparation.

g. Ensure that threats to security and security incidents pertaining to classified information, including foreign government information (FGI), are reported, recorded, coordinated with the proper authorities, and, when necessary, investigated and that appropriate action is taken to mitigate damage and prevent recurrence. Ensure that incidents involving the loss or compromise of classified material as described in DoDM 5200.01 are immediately referred to the cognizant investigative authority. In cases where compromise is determined or cannot be ruled out, ensure that security reviews and other required assessments are conducted as soon as possible. Coordinate with local information assurance officials, but retain responsibility for inquiries into incidents involving possible or actual compromise of classified information resident in or on IT systems.

h. Maintain liaison with the activity public affairs officer or information security officer, as appropriate, and the operations security (OPSEC) officer to ensure that information, including press releases and photos, proposed or intended for public release, including via website posting, is subject to a security review in accordance with DoDD 5230.09 (Reference (r)), DoDI 5230.29 (Reference (s)), and Deputy Secretary of Defense Memorandum (Reference (t)).

i. Coordinate with other activity officials regarding security measures for the classification, security containerguarding, transmission, declassification, and destruction of classified information.

3. The agency security assistant is responsible for the following areas:

Name:	Building Number:
Mobility	511
K-9	3340

4. If you have any questions, please contact _____at 654-XXXX or by e-mail at XXX.

JOHN A. DOE, Col, USAF
Agency Commander

Attachment 3

FOR OFFICIAL USE ONLY

SAMPLE SAFE CUSTODIAN APPOINTMENT MEMORANDUM

(USE GOODFELLOW AFB FOUO/PII LETTERHEAD STATIONARY)

DATE

MEMORANDUM FOR 17 TRW/IP

FROM: Agency/Office Symbol

SUBJECT: Security Container Custodian Memorandum

1. The following is a listing of authorized security containers and appointment of security container custodians for each security container residing in the (agency).

Security container	Manufacturer/Model	Lock Type	Serial Number	Bldg/Rm
SFS # 1 –	Mosler/SF-C2/2-dr	X-07	123456	Bldg 3332 Rm 17
SFS # 2 –	Hamilton/XX-C4/4-dr	X-09	0987655	Bldg 3324 Rm 4
SFS # 3 –	Mosler/SF-C2/2-dr	X-07	7586943	Bldg 2424 Rm 1

	Rank/Name	Office Symbol	Phone	Clearance
SFS #1				
Primary:	GS-09 Sara Conners	17 SFS/S3	654-3510	Secret
Alternate:	TSgt Michael Havannah	17 SFS/S3	654-3509	Secret

SFS #2
Primary:
Alternate:

2. A copy of this listing is posted in the miscellaneous section of the Security Assistant Handbook. If you have any questions please contact Name, Security Assistant at 654-XXXX.

JOHN A. DOE, Col, USAF
Unit Commander

The information herein is For Official Use Only (FOUO) which must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties