BY ORDER OF THE COMMANDER
MCCONNELL AIR FORCE BASE (AMC)

MCCONNELL AIR FORCE BASE
INSTRUCTION

16-1401

27 APRIL 2023

Operations Support

INFORMATION PROTECTION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 22 ARW/IP

Certified by: 22 ARW/DS
(Mr. Russell W. Rumley)
Pages: 12

This publication implements DoDM5200.01_AFMAN16-1404, (Vols 1-3), *Information Security Program*, DoDM5200.02_AFMAN16-1405, *Air Force Personnel Security Program* and DoDM5220.22_AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*. It provides guidance and procedures for managing and executing the wing's Information Protection programs at all levels and assigns specific responsibilities to commanders, unit security assistants and classified custodians. It is applicable to all 22d and 931st Air Refueling Wing units and all host and tenant units serviced through agreements by the 22 ARW Information Protection Office. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAFMAN 90-161, *Publishing Processes and Procedures,* for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, Records Management and Information Governance Program and are disposed in accordance with the Air Force Records Disposition Schedule, (RDS) which is located in the Air Force Records Information Management System (AFRIMS).

1. Overview. Information Protection. Information Protection (IP) is a subset of the Air Force Security Enterprise. Information Protection consists of a set of three core security disciplines (Personnel, Industrial and Information Security) used to:

1.1. **Protect classified information that, if subject to unauthorized disclosure, could.** reasonably be expected to cause damage to national security. Protect Controlled Unclassified Information (CUI) which may be withheld from release to the public. (Information Security).

1.2. **Determine military, civilian and contractor personnel's eligibility to access classified.** information or occupy a sensitive position. (Personnel Security).

1.3. **Ensure the protection of classified information that may be released or has been released.** to current, prospective, or former contractors, licensees, or grantees of United States agencies. (Industrial Security).

2. Program Management Roles and Responsibilities.

2.1. **Vice Commander.** The Vice Commander, 22d Air Refueling Wing (22 ARW/CV), is delegated the authority to act as Head of the Activity in order to ensure security controls, safeguards and countermeasures are established through application of risk management principles, as appropriate for the 22 ARW and those tenant unit/organizations with a support agreement outlining Information Protection requirements.

2.2. **Chief of Information Protection.** The Chief, Information Protection (CIP), (22 ARW/IP) executes the information protection program on behalf of the wing commander and provides oversight and direction to group and squadron commanders, directors, activity security managers, assistant security managers, security assistants and the security specialists assigned to the Wing Information Protection Office.

2.2.1. The CIP shall report to the 22 ARW/CV.

2.2.2. The CIP is delegated the authority to certify and revalidate secure rooms (i.e. open storage areas) as required.

2.2.3. The CIP will host a Security Assistant meeting at least once every six months and prepare meeting minutes to be distributed to participants and commanders.

2.3. **22d Civil Engineer Squadron (22 CES):**

2.3.1. 22 CES/Structures (22 CES/CEOHS). Will provide engineering support as needed to evaluate and certify construction standards for secure room/open storage areas.

2.3.2. 22 CES/Explosives Ordinance Disposal (22 CES/CED). As the entity with the primary requirement for access to Restricted Data and Controlled Nuclear Weapons Design Information, the 22 CES/CED Flight Chief is designated as the Restricted Data Management Official IAW DoDM 5200.01V1_AFMAN16-1404V1.

2.4. **22d Security Forces Squadron (22 SFS).** 22 SFS/Plans and Programs (S5) is the POC for all Intrusion Detection Systems (IDS) related issues, to include estimates for new installations, changes to existing systems, certifications and maintenance. 22 SFS/S5 will provide support as needed to evaluate and certify alarm system for secure room/open storage areas.

2.5. **Commanders, Directors and Staff Agency Chiefs.** Commanders, Directors and Staff Agency Chiefs (referred to from here on as commanders):

2.5.1. Will appoint a primary Security Assistant (SA) who is a U.S. citizen and has a security clearance which allows access to the highest level of material the unit possesses. Submit SA appointment memorandums to 22 ARW/IP. Include full name, rank/grade, organization, office symbol, phone number and clearance level using the template provided by 22 ARW/IP. When a change occurs, a new appointment letter should be submitted to 22 ARW/IP within 10 duty days.

2.5.1.1. Should appoint at least one alternate SA who is a U.S. citizen and has a security clearance which allows access to the highest level of material the unit possesses. Alternate SA should be included on the same memorandum as primary SAs and are required to meet the same qualifications.

2.5.1.2. Due to the amount of training required and the scope of duties, commanders should ensure personnel assigned as SAs are available for at least 12 months. It is recommended personnel pending retirement, permanent change of station or medical discharge are not considered for these duties.

2.5.2. Will designate and approve classified reproduction equipment by posting a visual aid on the machine that states its approval to be used for classified reproduction. All other machines with copying capability will be posted with a visual aid that indicates they are not approve for classified reproduction. Classified reproduction will not be approved/authorized for copiers connected to the unclassified network. Classified reproduction will not be approved/authorized for copiers with an internal hard drive unless they are located within an approved open storage area.

2.5.3. Will ensure all (military, civilian and contractor) personnel in/out process through the SA by including the SA as a mandatory item on the organizations in/out processing checklist.

2.5.4. Will comply with the guidance in **Paragraph 4** of this instruction when considering new secure room/open storage facilities.

2.5.5. Will notify 22 ARW/IP and 22 SFS/S5 of modifications to existing vaults and secure rooms to ensure changes do not affect secure room or alarm systems certification.

2.5.6. Will provide information and data as requested by the IP office to support data taskings and execution of the IP programs.

2.6. **Security Assistants.** Implement and monitor the Information, Personnel and Industrial Security Programs within the unit on behalf of the unit commander and the Wing Activity Security Manager. SAs will:

2.6.1. Complete initial SA training within 90 days of appointment. SA training will be conducted through a combination of on-line courses and local classroom training. 22 ARW/IP will provide newly appointed SAs a listing of currently required on-line courses that must be completed before attending local classroom training. Local classroom training will be offered monthly.

2.6.2. Accomplish the following in-processing actions with all newly assigned military, civilian and contractor personnel:

2.6.2.1. Provide or direct assigned personnel to accomplish initial Information Security training, Controlled Unclassified Information training, Derivative Classification training and Personnel Security briefings as appropriate for the persons assigned duties. Establish methods to document and track completion of this training.

2.6.2.2. Establish ownership in the Joint Verification System (JVS), or its successor system.

2.6.2.3. Ensure each cleared person in their unit has signed an SF 312, *Non-Disclosure Agreement* and that it is documented in JVS.

2.6.2.4. Once training is complete, document classified access in JVS at the level required for the position they occupy on the unit manning documents, or, for contractors, the level specified by the DD Form 254, *Department of Defense Contract Security Classification Specification.* Classified access will match the access required to perform official duties and not necessarily the eligibility level listed in JVS.

2.6.3. Ensure all personnel with access to classified security containers and secure rooms have documentation showing completion of Classified Custodian training. A Classified Custodian training presentation is available on the 22 ARW/IP SharePoint site.

2.6.4. Complete and post "Your Security Assistant is" signs throughout areas of responsibility. An example sign is available on the 22 ARW/IP SharePoint site.

2.6.5. Ensure at least one SA or a representative of the unit attends meetings hosted by the IP office. Geographically separated units will attend in-person when feasible or at lease via other electronic means.

2.6.6. Provide information and data as requested by the IP office to support data taskings and execution of the IP programs.

2.6.7. Establish and maintain a unit program binder as outlined in **paragraph 5.8** below.

2.7. **Classified Custodians.** The first two names listed on the SF 700, *Security Container Information*, are designated the "Safe Custodians" and are responsible for container security serviceability, preventive maintenance and contents of containers, vaults and secure rooms. A contractor may not be a custodian.

2.7.1. Custodians will conduct visual inspections of containers, vaults and locks on secure rooms upon initial purchase of a container or initial establishment of a secure room and at least every 5 years thereafter. Visual inspections will be accomplished using the checklist at Appendix 2 to Enclosure 3, of DoDM5200.01V3_DAFMAN16-1404V3 and documented on the Optional Form (OF) 89, *Maintenance Record for Security Containers/Vault Doors*.

3. Classified Storage.

3.1. **Personal Control and Observation.** Classified information is required to be either under the personal control and observation of an authorized person, stored in a GSA approved locked security container, or in a certified vault/secure room. Personal observation and control is defined as having sufficient surveillance and physical control over classified information to detect and prevent access by unauthorized persons. While eyes on observation and physical possession are the ideals, common sense risk management options may be utilized to meet the

intent of protecting classified information while accomplishing the mission. For example, a classified workspace with only one entrance, depending on the physical environment, could potentially be protected if a cleared person was in close enough proximity to maintain observation and control over the only entrance. Such risk management decisions should be made at the appropriate leadership level (i.e. the work center supervisor) for the area and the options used shall be appropriate to the environment in which access occurs and considerate of the nature, volume and availability of the information.

3.2. **Risk Assessment and Security-in-Depth.** Risk assessments have been accomplished that measure both the current threat and vulnerabilities for McConnell AFB. The information from these assessments and the existence of multiple layers of defense, including perimeter fencing, 24/7 installation entry control and roving Security Forces patrols with the ability to respond to any facility on base within 5-10 minutes, have resulted in the determination that security-in-depth exists for all facilities on McConnell AFB.

3.3. **Overnight Storage.** The Installation Commander has designated the McConnell AFB Command Post, as the overnight repository for classified material and is the designated storage facility for transit or emergency storage of collateral classified information/material up to the TOP SECRET level.

3.4. **Emergency Plans.** Emergency plans for the protection of classified shall be readily available at all security containers, secure rooms and vaults. A sample Emergency Plan is available on the 22 ARW/IP SharePoint site.

3.5. **Collateral classified containers.** Collateral classified containers will be marked with a unique identifier that will be recorded on the unit's container listing. If the manufacturers serial number is not used, mark the container with a unit/number combination on the front upper left or right corner (example: SFS-01; MXS-02; FSS-03). Marking with a permanent marker will suffice.

3.5.1. The Information Security Program Manager is a GSA-certified technician/inspector who can perform limited container/lock maintenance and repair or confirm authorized penetration and repair methods have been used by off-base locksmiths in order to validate the integrity of GSA approved equipment. Services of off-base locksmiths are the financial responsibility of the owning unit.

3.5.2. If a security container is no longer going to be used or is being placed in storage, it will be closely examined for classified material, the combination will be set to the default (50-25-50) and a notice shall be attached to the container stating, "Out of Service". If a container is no longer needed, contact 22 ARW/IP to coordinate the transfer of the container to a unit who may have a need before turning a serviceable container into the Defense Reutilization Management Office. Do not remove the OF 89, *Maintenance Record for Security Containers/ Vault Doors.*

3.6. **Classified Processing Areas.**

3.6.1. For existing areas not meeting Secure Room requirements, but which are used for classified processing (i.e., SIPRNet, or other classified systems located in non-open storage areas) written procedures will be in place and available to aid users. The procedures may be incorporated into the unit security plan/instruction or may be published separately and a single plan may be used for multiple areas within the unit. As a minimum the procedures

(a User Checklist suffices) should address activation and deactivation procedures, rules for continuous observation, any required warning signage, details addressing prohibited items such as Personal Electronic Devices (PED), cameras, USB thumb drives, video recording devices, wireless devices and required physical security requirements. Include procedures for clearing a printer, if applicable. If windows afford visual observation of classified activities, drapes or curtains must be available and will be closed as needed. Locations of classified computer systems must be listed on the Standard Form (SF) 701, *Activity Security Checklist*, to ensure the end-of-day check includes verifying classified hard drives, laptops, TACLANE keys, etc., have been removed and properly stored in the security container. A sample security plan is available on the 22 ARW/IP SharePoint site.

3.6.2. All media and information technology equipment in the room must be marked to indicate whether it is classified, unclassified, or can be used to process classified. With the exception of protective cases that hold classified CDs/DVDs, only media that actually retains or stores classified information should be marked as classified. For example, a printer used to print classified information that does not retain the information should be marked as "authorized for use with classified information" but would not be marked as classified. Classified media storage cases and sleeves will be marked on all sides equal to the media contained within. A permanent marker may be used to annotate this information on a classified CD-ROM or DVD in lieu of the SF Medial Labels. Utilize and annotate SF 711, *ADP Data Descriptor Label*, or locally devised label, with the following: unit, office symbol, phone number if the media is removed from the office where it was created. Monitors do not have to be marked if a banner is present when the system is powered on.

3.6.3. The location of all classified resources will be listed on the SF 701 to ensure laptops, hard drives, TACLANE keys, other storage media and containers have been secured. Maintain a copy of each completed SF 701 on file for 30 days.

4. New Secure Rooms/Open Storage Areas. A multi-disciplined approach is required in the planning and construction of secure rooms/open storage areas. In order to ensure the finished product meets all the required standards, units considering establishing new facilities must include 22 ARW/IP, 22 SFS, 22 CES and 22 CS throughout the process.

4.1. **When construction is complete, a final survey will be accomplished by 22 ARW/IP with assistance as necessary from 22 CES/CEOHS and 22 SFS/S5 in order to certify construction and alarm standards meet the requirements of Department of DoDM 5200.01V3_DAFMAN 16-1404V3, *Information Security Program: Protection of Classified Information*, Appendix to Enclosure 3.** Once it is determined the room or vault meets all requirements, the CIP will provide the unit with a certification letter. The certification letter will be displayed on the inside of the main entry door to each approved open storage area. NOTE 1: Secure rooms/open storage areas certified and approved prior to this publication are not required to be re-certified/approved based solely on the publication of this instruction. NOTE 2: Open storage will not be approved solely for convenience.

4.2. **The secure room owner will prepare and submit a security plan/instruction for the secure room prior to final certification.** The security plan or instruction may be incorporated into the unit security plan/instruction or may be published separately and a single plan may be used for multiple secure rooms within the unit. If published separately, as a minimum, the plan will specify the area/location, reason for open storage, risk assessment determinations,

responsibilities, access and circulation controls to include related Entry Authority List (EAL) and visitor procedures, physical security and alarm check and maintenance requirements, required warning signage requirements, appropriate procedures associated with the OF 89, *Maintenance Record for Security Containers/Vault Doors*; the SF 702, *Security Container Check Sheet*; the SF 701; the SF 700, Security Container Information sheet; and details addressing prohibited items such as PEDs, cameras, USB thumb drives, video recording devices and wireless devices. The plan must be approved/signed by the unit commander, director or agency chief and made accessible and familiar to personnel using the area. A sample plan is available on the 22 ARW/IP SharePoint site.

5. Program Operations and Administration.

5.1. **Annual Clean-out.** The first duty day in the month of April is designated as the classified clean-out day. In addition to focusing on disposing of unneeded classified material, commanders, directors and staff agency chiefs will ensure all classified holdings are reviewed for required markings, possible downgrading and declassification. Units will document this action with a memorandum for record.

5.2. **Program Reviews.** The IP office is authorized to conduct an annual Information Protection Program Review (IPPR) of those 22 ARW units, tenant units and organizations with a Host Tenant support agreement aligning under the 22 ARW/IP Office. The CIP may elect to use a staff assistance visit (SAV) or Wing Inspection Team (WIT) event in lieu thereof. The CIP may also extend the annual requirement due to operational, scheduling or other factors as deemed warranted.

5.2.1. 22 ARW/IP will provide an IPPR report to the commander or director and SA of the unit after each review. The report will indicate whether discrepancies found are of a nature that warrants a follow up review to ensure corrective actions/measures are taken. The decision to conduct a follow-up review rests solely with the Information Protection office. If a follow-up is warranted, it will be conducted approximately 60 days after the IPPR or earlier at the unit's request.

5.2.2. Units will ensure that non-compliant items found during an IPPR from applicable Management Internal Control Toolset (MICT) checklists are entered and tracked as observations per AFI 90-201, *The Air Force Inspection System*.

5.3. **Classified Meetings.** Classified meetings will be conducted using the guidance in DODM 5200.01V3_DAFMAN16-1404V3. Standard, recurring and/or day-to-day classified mission meetings need not be continuously or formally approved. A classified meeting shall be formally approved by the appropriate commander, director, or agency chief if it can be deemed unique, complex and/or is a 'hosted' type event or meeting, especially when involving multiple organizations with non-unit attendees/visitors. The awareness thereof or attendance by senior leadership shall suffice for implied approval. All personnel holding classified meetings should utilize the Classified Meeting Checklist at Appendix 1 to Enclosure 2 of DoDM5200.01V3_DAFMAN16-1404V3.

5.4. **End-of-Day checks.** End-of-day checks will be accomplished every duty day in all areas that store or process classified. As much as practical, each classified component (computer, hard drive, container, SIPR terminal, CIK key etc.) should be listed individually on the SF 701, Activity Security Checklist, to ensure all items are secured at the end of the day. A fillable

electronic version of the SF 701 is available from the **www.GSA.gov** website. Maintain each completed SF 701 for 30 days to assist with inquiries into Information Security Incidents. In addition to filling out the SF 701, the person conducting the End-of-day checks will annotate the "Checked By" column of the SF 702, Security Container Check Sheet, for each container. Maintain each completed SF 702 on file for 30 days to assist with inquiries into Information Security Incidents.

5.5. **Shredders.** All shredders will be marked to indicate they are approved for destruction of classified information. Documentation that shows the device is listed on the National Security Agency's (NSA) evaluated products listing should be kept with the shredder.

5.6. **Hand-Carrying Classified.** Hand-carrying of classified will be minimized to the greatest extent possible. Permission to hand-carry classified within the confines of McConnell AFB requires only the awareness of an immediate supervisor. Classified cover sheets will be used at all times and an unmarked outer wrapper, envelope, folder, or case will be used to conceal the fact that classified is being carried. IAW DoDM5200.01V3_AFMAN16-1404V3, a DD Form 2501, *Courier Authorization Card*, or authorization letter is required to hand-carry classified off-base and all off-base couriers will receive and acknowledge a briefing from the SA.

5.7. **Mail Handling.** Treat and protect all unopened accountable correspondence as classified until the contents are determined to be unclassified. Accountable correspondence consists of First Class (marked "Return Service Requested"), Registered and Certified U.S. mail and overnight deliveries from authorized GSA carriers such as FedEx and UPS. This correspondence must be stored in a GSA-approved security container if unopened, until hand delivered to the addressee, or opened to determine the contents. Unattended accountable correspondence found to contain classified will be reported to 22 ARW/IP as a security incident.

5.8. **Security Clearance Applications.** 22 ARW/IP will task security clearance applicants with a 14-day suspense to complete electronic submission of the required forms. Failure to complete the submission within the 14-day window will require a re-initiation request from the unit Security Assistant. Failure to complete the submission more than twice will require a re-initiation request from the unit Commander. Additional failures to complete the application will require a memorandum with explanation, from the next command level. At each missed suspense COMMAND should consider initiating a Continuous Vetting Incident Report if it is felt the cause of the failure to complete is the applicant's reluctance to divulge derogatory information.

5.9. **Program Binders.** Maintain an Information Protection program binder. Use of the unit "e-binders" on the 22 ARW/IP SharePoint site is encouraged but not mandatory. These binders serve as an environmentally friendly option that allows documentation to be secured through permissions, while remaining available to both the unit program managers as well as the IP staff. Regardless of the type of binder used, the following items should be maintained and/or made available upon request.

5.9.1. Appointment letters and training documentation for SM, ASM and SAs as required.

5.9.2. Unit internal operating instructions and/or written plans, as applicable.

5.9.3. List of security containers within the organization, showing manufacturer, class, number of drawers, unique container ID#, lock type and location. The list must also contain all vaults and secure rooms approved by the CIP. Memos listing custodians and names of persons having knowledge of the combinations. Documentation of training covering classified safe operations for all personnel with access to the container.

5.9.4. Copies of the unit's IP program reviews, inspection, or review reports. Maintain last two years, to include documentation of corrective actions if not recorded elsewhere.

5.9.5. Copies of signed AF Forms 2587, Security Termination Statement. Maintain for 2 years in accordance with the AFRIMS RDS.

5.9.6. Copies of AF Forms 2583, *Request for Personnel Security Action*, for submitted security clearance investigations and interim or final access to special accesses such as Restricted Data (RD), Critical Nuclear Weapon Design Information (CNWDI), or North Atlantic Treaty Organization (NATO). Maintain until access is no longer required.

5.9.7. Training documentation, to include initial and refresher training. Maintain records for two years.

5.9.8. Copies of any letters approving classified reproduction equipment that are posted with the device.

5.9.9. Miscellaneous other documentation to include annual position code review memos, cleanout day memos, secure room certification paperwork, etc.

5.9.10. Industrial Security program documentation such as the DD Form 254, *Department of Defense Contract Security Classification Specification*, Performance of Work Statements and contractor Visit Requests.

GEORGE N. VOGEL, Colonel, USAF
Commander, 22d Air Refueling Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDM5200.01V1_AFMAN16-1404V1, *Information Security Program: Overview, Classification and Declassification*

DoDM5200.01V2_AFMAN16-1404V2, N16-1404V2, *Information Security Program: Marking of Classified Information*

DoDM5200.01V3_DAFMAN16-1404V3, *Information Security Program: Protection of Classified Information*

DoDMAN5200.02_AFMAN16-1405, *Air Force Personnel Security Program*

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

Prescribed Forms

None

Adopted Forms

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

DD Form 2501, *Courier Authorization Card*

OF 89, *Maintenance Record for Security Containers/Vault Doors*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

Abbreviations and Acronyms

AFRIMS—Air Force Records Information Management System

CIP—Chief of Information Protection

CUI—Controlled Unclassified Information

EAL—Entry Authority List

IP—Information Protection

IPPR—Information Protection Program Review

IDS—Intrusion Detection System

JVS—Joint Verification System

MICT—Management Integrated Control Toolset

NSA—National Security Agency

POC—Point of Contact

RDS—Records Disposition Schedule

SA—Security Assistant

TACLANE—Tactical Local Area Network Encryption device

Office Symbols

22 ARW/CV—Vice Commander, 22d Air Refueling Wing

22 ARW/IP—Information Protection Office, 22d Air Refueling Wing

22 CES/CED—Explosives Ordinance Disposal flight, 22d Civil Engineer Squadron

22 CES/CEOHS—Structures flight, 22d Civil Engineer Squadron

22 SFS/S5—Plans and Programs flight, 22d Security Forces Squadron

Terms

Classified Custodian—An individual tasked with responsibility for the proper operation and maintenance of a container, vault or secure room.

Classified Processing Area—An area where classified is stored, handled or processed.

Controlled Unclassified Information—Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations and government-wide policies.

Critical Nuclear Weapons Design Information—Classified Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device.

Formerly Restricted Data—Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as Restricted Data.

NSA Evaluated Products listing—A list of devices that have passed evaluation by meeting requirements set by the NSA for the destruction of classified information.

Open Storage Area—An area approved by the Wing Commander (or as delegated) for open storage of classified information. An open storage area must meet Secure Room requirements.

Ownership—A direct relationship in JVS between a person and the Security Management Office

Restricted Data—All data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but not data declassified or removed from the Restricted Data category pursuant to section 2162 of The Atomic Energy Act of 1954, as amended.

Secure Room—An area constructed in accordance with the requirements of the Appendix to Enclosure 3 of DoDM5200.01V3_AFMAN16-1404V3. Secure rooms are created when the size

and nature of the classified material, or operational necessity make the use of GSA approved containers unsuitable or impractical.