BY ORDER OF THE COMMANDER
505TH COMMAND AND CONTROL WING

505 CCW INSTRUCTION 31-2

25 February 2010

Security

SECURITY OPERATING PROCEDURES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSABILITY: This publication is available digitally on the 505 CCW Publications Management SharePoint Team Site at https://ccw.hurlburt.af.mil/sites/CC/DP/505%20CCW%20Publications%20Management/default.aspx . Forms are available on the e-Publishing website at http://www.e-publishing.af.mil/ or http://www.af.mil/e-publishing/index.asp for downloading

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 505 TRG/SF

Certified by: 505 TRG/CC
Col Christopher DiNenna
Pages: 26
Distribution: F

This Operating Instruction implements portions of DoD 5200.1-R, *Information Security Program*, January 1997; DoD 5200.2-R, Personnel Security Program, January 1987; DoD Administrative Instruction 26, *Information Security Supplement to DoD 5200.1-R* April 1987; DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*, April 1997; AFI 31-401, *Information Security Program Management*, 1 November 2005; AFI 31-501, *Personnel Security Program Management*, January 2005; and AFI 31-601, *Industrial Security Program* Management, June 2005. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123 (will convert to AFMAN 33-363), *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil.** This instruction does not supersede the above instructions, but clarifies procedures specific to 505 CCW operations. This instruction applies to all 505 CCW military, DoD civilian, contractor, and TDY personnel involved in the development, instruction, presentation, attendance, or support of 505 CCW training, courses, conferences, exercises and other major events.

SECURITY OPERATING PROCEDURES

SUMMARY OF CHANGES

1. Updated issue dates for AFI's 31-401, 31-501, 31-601. Removed references to CCW OI 31-4 due to obsolescence.

2. Added TDY personnel to applicability of this OI.

3. Added squadron commanders to paragraph 1.2.1.

4. Added physical security to paragraph 1.2.1.1.

5. Changed Security Infractions to Security Deviations in paragraph 2.2.5.2.

6. Clarified paragraph 3.2.6., Marking Briefings.

7. Changed paragraph 3.2.7., Marking Magnetic Media, to read "approved media."

8. Renamed paragraph 3.10 to Computer and Network Security, consistent with current guidance. Clarified responsibilities.

8. Added paragraph 3.12., Portable Electronic Devices.

9. Clarified paragraph 5.5.1.3, adding instructions to spin the lock dial and check the handle when performing end-of-day security checks.

10. Changed the requirement for monthly physical security sweeps to quarterly, added assistance by Wing Security office as required. Added Security Forces notification requirement prior to starting physical security sweeps.

11. Added paragraph 7.2.2., requirement and instructions to utilize Event Media/Electronics Exception Letter for exercises, events, and conferences.

Chapter 1

BASIC POLICY AND RESPONSIBILITIES

1.1. Purpose:

1.1.1. This instruction establishes basic security policies and procedures for 505 CCW military, DoD civilian and contractor personnel. This living document is intended to present an overview of the security procedures and requirements contained within applicable directives and manuals. It is incumbent upon all personnel to read, understand and adhere to the procedures contained in this instruction to ensure all classified material is properly protected, stored, handled, labeled, transmitted, inventoried and destroyed.

1.1.2. Presidential Executive Orders, DoD directives and AF instructions provide general security policies/procedures. These instructions (including local security guidance) have been compiled and modified to ensure 505 CCW-hosted exercises, experiments, training, conferences, major events, as well as day-to-day operations meet security criteria. The 505 TRG Security Forces (SF) and your unit Security Manager (SM) can provide personnel with further information and instructions.

1.1.3. Since 505 CCW programs contain information deemed vital to national security, it is imperative all classified and proprietary information/materials received or generated be afforded a degree of protection commensurate with its classification in accordance with federal directives. This requires the combined efforts of all individuals who utilize classified materials and systems. The key to success for this security program is vigilance, training, awareness and the acceptance of individual security responsibilities.

1.2. RESPONSIBILITIES:

1.2.1. The Wing commander, as well as individual squadron commanders, bear overall responsibility for their security programs and ensure the following:

1.2.1.1. Security programs are sufficiently staffed and equipped to support information, personnel, industrial, force protection and antiterrorism, foreign disclosure, physical, and operations security programs.

1.2.1.2. Security personnel are afforded adequate training opportunities to maintain compliance with security guidance.

1.2.1.3. Security personnel are empowered to ensure security compliance at wing and subordinate unit levels.

1.2.2. All 505 CCW personnel are responsible for safeguarding classified materials under their control. The 505 TRG/SF and unit SMs are appointed to oversee day-to-day security

operations and assist with group and squadron-level security programs as required for the overall success of the security program. 505 TRG/SF and local SMs will administer and direct security policies as outlined in this instruction and other guidance. Specifically, 505 TRG/SF and your unit SM are responsible for the following:

1.2.2.1. Ensure suitable protective measures are established and available for all classified and unclassified/sensitive material(s) used in support of 505 CCW activities. This includes force protection measures, resource protection methods and other established procedures.

1.2.2.2. Ensure all clearances are validated, personnel are badged and properly coded for their appropriate access level, and cleared personnel with a need-to-know have access to information or locations in support of the 505 CCW mission. Integrate a strict need-to-know policy to further support classified and unclassified activities.

1.2.2.3. Provide 505 CCW personnel with quarterly security education and refresher training through electronic means. Continually stress the importance of personal responsibilities for protecting classified information and equipment.

1.2.2.4. Ensure document control procedures are established for hard-copy documentation, magnetic media and automatic information systems (AIS) hardware IAW applicable security guidance. Ensure these procedures are integrated into daily and event-centric activities.

1.2.2.5. Provide an Emergency Actions Plan (EAP). Outline procedures for safeguarding classified information during natural or man-made disasters, incidents, emergency situations and designating safe evacuation routes to include gathering locations (when applicable).

1.2.2.6. Perform semiannual security self-inspections to ensure compliance with security instructions.

1.2.2.7. Maintain this instruction to ensure assigned personnel are familiar with and review its contents annually by utilizing electronic means to include email read receipts as a method to document compliance.

Chapter 2

PERSONNEL SECURITY

2.1. General:

2.1.1. The core aspect of the security plan is personnel security. This involves the careful selection of personnel for access, indoctrination and continued reiteration of security responsibilities to achieve the highest level of security consciousness and practice on the part of each individual.

2.1.1.1. Access to classified information or material is neither a right nor an entitlement. It is a wholly discretionary security determination granted only to personnel who have a valid need to know. Those personnel must meet background standards set forth by Department of Defense and Air Force policy to determine trustworthiness. The 505 CCW/CC, group commander, and squadron commanders are responsible for making this determination based on a review of personnel and medical records and local police and agency checks. Based on the nomination made by the 505 CCW Commander, group commander, or squadron commanders, confirmation of eligibility by the 505 TRG/SF or local SM, individuals are granted access to classified information, material and/or facilities.

2.2. INDIVIDUAL REPORTING REQUIREMENTS:

2.2.1. The number of espionage cases over the last few years has highlighted gaps in DoD's security clearance programs. Although reporting procedures have not changed, a tougher stance is being taken concerning the enforcement of current directives and instructions. Personnel will be subject to increased scrutiny regardless of their periodic reinvestigation requirement. Previously, security incidents and/or personal shortfalls (i.e., reckless driving, Driving Under Influence, bad checks or Article 15s) were only reported during a periodic reinvestigation. IAW DoD Continued Evaluation policy, current directives require individuals to report incidents to your security staff in a timely manner, even if they are not currently due for a periodic review. Security managers will work closely with commanders and first sergeants to ensure compliance with these established efforts. All 505 CCW personnel need to be diligent in reporting any changes to their status to include marriage and/or divorce.

2.2.2. The activities listed below must be reported to your SM by the most expeditious means and followed up in writing, if required. The 505 TRG/SF and local SMs will report these activities up their appropriate security chain as required. Failure to comply or attempts to hamper reporting requirements may adversely affect an individual's continued eligibility for access regardless of current position or title.

2.2.2.1 Changes in Personal Status: Personnel must notify the 505 TRG/SF or SM of any significant changes in their personal status. Significant changes include, but are not limited to, the following:

2.2.2.2. Change in marital status: Changes in marital status include marriage, intent to marry, or marriage to a foreign national, divorce, or proposed name change. Cohabitants are treated as spouses in this context. Marriage to a foreign national can be grounds for reevaluation of access eligibility.

2.2.2.3. Change of duty assignment: A change of duty assignment may affect the need-to-know for continued access to classified information. When it is determined an individual no longer requires access, immediately notify your SM in order to terminate any pending investigative actions and complete an AF FM 2587, Security Termination Statement, for the individual as required. This will help reduce the cost and lost time caused by an unnecessary investigation.

2.2.2.4. Other significant changes include, but are not limited to, command-directed counseling by mental health agencies, credit judgments, bankruptcy filing or repossessions, and adverse involvement with law enforcement agencies, including arrests for driving while under the influence, reckless driving and driving while intoxicated and traffic violations of $150 or more.

2.2.2.5. Additional Off-Duty Employment. Potential conflict may arise between an individual's responsibility to protect classified information and any outside employment or other activity from contact or association with foreign nationals.

2.2.3. Foreign Travel. Foreign travel must be reported to your local SM and/or Office of Special Investigations (OSI) not later than five (5) duty days in advance of official travel, twenty (20) duty days in advance for personal travel and thirty (30) duty days in advance of travel to a country identified on the FBI's classified national security threat list. Upon returning from foreign travel, report back to your SM and/or OSI any of the following:

2.2.3.1. Contact with personnel from foreign diplomatic establishments.

2.2.3.2. Recurring foreign contact when financial ties are established or involved.

2.2.3.3. Contact with an individual under circumstances that suggest traveler may be the target of an attempted exploitation by the intelligence services of another country.

2.2.3.4. Unusual incidents considered threatening or suspicious.

2.2.3.5. Social contact with a foreign national when:

2.2.3.5.1 An individual is questioned regarding the specifics of your job.

2.2.3.5.2. Questioning is persistent regarding professional interest, social obligations or family situations.

2.2.3.5.3. Frequent or continuing contact is anticipated.

2.2.4. Adverse Information. Any adverse information obtained concerning personnel, members of their immediate families (spouse, children, brothers, sisters, mother and father), or those who are in the process of being approved for access, could affect the individual's suitability for initial or continued access to classified. Information that should be reported includes, but is not limited to:

2.2.4.1. Disloyalty to the United States.

2.2.4.2. Evidence or indications of moral turpitude.

2.2.4.3. Excessive and/or illegal use of intoxicants or drugs.

2.2.4.4. Lack of honesty, integrity or discretion.

2.2.4.5. Serious financial difficulties.

2.2.4.6 Emotional instability or any character defect or problem that could subject the individual to blackmail, pressure or coercion.

2.2.5. Security Incidents.

2.2.5.1. Security Violation. Any incident involving the loss, compromise or suspected compromise of classified information must be reported to your unit SM, wing security office, or host base Security Forces information security program manager within 24 hours of identification.

2.2.5.2. Security Infraction. Any incident not in the best interest of security that does not involve the loss, compromise or suspected compromise of classified information will be documented by your 505 CCW Security Staff and forwarded to the host base information security program manager and made available for review during the next security review.

2.2.5.3. Inadvertent Disclosures. Any involuntary unauthorized access to classified information by an individual without access is an inadvertent disclosure. Individuals involved will be interviewed by your 505 CCW Security Staff to determine the extent of exposure and requested to complete an Inadvertent Disclosure Statement.

Inadvertent Disclosure Statements will be forwarded from the 505 CCW Security Staff to the appropriate agency within 24 hours of the incident.

2.2.6. Other Reportable Incidents.

2.2.6.1 Any attempt by representative(s) of a government, agency or department seeking or threatening scrutiny of areas/assets with reviews, security cognizance, inspections, etc.

2.2.6.2. A change, modification or relocation of physical/technical security in areas used for classified activities.

2.2.6.3. Any attempt by a representative of the media or general public to obtain classified information or details.

2.2.6.4. Information concerning espionage, sabotage or subversive activities directed against 505 CCW personnel or facilities that would jeopardize activities or participants.

2.2.6.5. Any actual or suspected attempt by foreign interests to gain access to classified information.

2.2.6.6. Any emergency condition rendering 505 CCW personnel unable to provide adequate protection of classified information or material.

2.3. Standard Form 312, Non-disclosure Agreements (NDA).

2.3.1. Signing the NDA is a prerequisite for obtaining access to classified information, once access is granted individuals will sign NDA as stated in, AFI 31-501, Personnel Security Program Management, and EO 12958, April 1995. Once signed by active military member, 505 TRG/SF will forward a copy to HQ AFPC/DPFFCMI, 550 C Street West, Suite 21, Randolph AFB TX 78150-4723, who will retain for 50 years.

2.3.2. For Air Force civilians, to the servicing civilian personnel office, HQ AFPC/DPCMP, 550 C Street West, Suite 21, Randolph AFB TX 78150-4723.

2.3.3. For DoD contractor employee who may not have been briefed by the company FSO due to location issues, 505 TRG/SF will forward a copy to the cognizant security agency listed on the company's DD FM 254.

2.3.4. All 505 CCW SMs will record the NDA in JPAS prior to 505 TRG/SF forwarding signed NDA for retention.

2.4. SCI Access.

2.4.1. The information below applies to Hurlburt Field units only (through para 2.4.9). All other 505 CCW units and detachments not at Hurlburt Field need to contact their unit SM or servicing SSO to determine local requirements.

2.4.2. All requests for access to Sensitive Compartmented Information (SCI) are processed through ACC and locally conducted by AFSOC/SSO. 505 TRS/SF will forward all appropriate correspondence to HQ ACC/SSO in reference to SCI indoctrination request.

2.4.3. An SCI pre-screening interview will be conducted on all personnel who are 30 days outside of their last periodic review (PR). The interview will be conducted by a government agent (military or GS-civilian) and forwarded to their applicable SCI monitor (SCIM), who in turn will forward the interview to ACC/SSO.

2.4.4. A justification letter and a prescreening interview, prescribed by DoD 5105.21-M-1, SCI Administrative Security Manual, DoD 5200.2R, Personnel Security Program, and AFI 31-501, Personnel Security Program will be conducted by the 505 TRG/SF office and forwarded to the ACC/SSO for approval.

2.4.5. A contractor's SCI access will not be transferred in status unless they are transferred within the company under the same contract number or they move to another company that is Government directed for awarded contract change. Supporting documentation of either circumstance is required with the transferred-in-status request (DD FM 30 or DD FM 254 from current company showing transfer under same contract or DD FM 254 from new company).

2.4.6. Unit SMs should contact 505 TRG/SF for dates and times SCI indoctrinations will be conducted. Mass indoctrinations are conducted by AFSOC/SSO on Fridays at 0930, unless otherwise notified. Compelling need cases will be considered on an individual basis. This office will assist in the coordination and completion of applicable paperwork.

2.4.7. Project officers or event leads for Hurlburt-based exercises, large-scale events, classes, conferences and meetings involving SCI must forward a list of non-Hurlburt participants to 505 TRG/SF as soon as possible. This will expedite local SSO confirmation of receipt of visit certifications for the event.

2.4.7.1. At a minimum, the participant list must include name, SSAN, organization or company, wing POC, and purpose and dates of visit.

2.4.8. Security managers will follow all local rules and guidance outlined by their servicing SSO. ACC/SSO has authority to grant our assigned personnel and visitors access to SCI information and/or facilities.

2.4.9. Urgent (one time, mission essential) and Compelling Need (immediate necessity) requests will be prepared by 505 TRG/SF and signed by the responsible unit CC or his designee. The wing SM will forward and monitor these requests for disposition.

Chapter 3

INFORMATION SECURITY

3.1. General:

3.1.1. Protecting classified information is critical in support of 505 CCW security programs and mission. The goal of Information Security is to efficiently and effectively protect all classified information and material; encourage and advocate the use of risk management principles; focus on identifying and protecting only that information which requires protection; integrate security procedures into our daily processes so they become second nature; and ensure all personnel understand their security roles and responsibilities and take them seriously.

3.1.2. Basic Information Security guidance and requirements are outlined in DoD 5200.1-R, Information Security Program, and AFI 31-401, Information Security Program Management. These documents, along with DoD 5200.1-PH, DoD Guide to Marking Classified Documents, provide the basic marking guidelines for all classified material.

3.1.3. Your local SM serves as the overall Information Security Manager for collateral activities conducted by your organization; however, all 505 CCW personnel are responsible for understanding the classification process, classification guidelines, marking and labeling requirements.

3.2. Classification and Markings:

3.2.1. Quality classification management is essential to maintaining the integrity of classified information and preventing compromise and/or unauthorized access. In order to readily identify classified information, the material must be conspicuously marked with the proper classification markings as soon as it is produced. Individuals generating classified documents or information are responsible for ensuring proper classification of all information contained within. Refer any questions or concerns to your local SM for clarification and/or assistance.

3.2.2. There are only two ways information is classified--originally or derivatively.

3.2.2.1 Original classification is an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Only individuals specifically authorized in writing by DoD component secretaries may classify documents originally.

3.2.2.2. Derivative classification is the incorporation, paraphrasing, restatement or generation in new form of information that is already classified, or the classification of information based on a classification guide from an Original Classification Authority (OCA).

3.2.3. There are three levels of classification: Confidential, Secret and Top Secret.

3.2.3.1. Confidential applies to information or material, which the unauthorized disclosure of which could be reasonably expected to cause damage to national security.

3.2.3.2. Secret applies to information or material, which the unauthorized disclosure of which could be reasonably expected to cause serious damage to national security.

3.2.3.3. Top Secret applies only to information or material which the unauthorized disclosure of which could be reasonably expected to cause exceptionally grave damage to national security.

3.2.4. Marking Requirements. Classification markings and applicable codewords/caveats must be conspicuously stamped, printed, written or affixed to all classified material. Classified material markings include: overall classification and portion markings; identity of originating agency and date; title or subject; classification source and downgrade or declassification instructions; copy and page numbers; document control number (Top Secret only); and distribution list, if applicable.

3.2.5. Marking Documents. Refer to DoD 5200.1-PH and any questions/concerns to your unit SM or 505 TRG/SF.

3.2.6. Marking Briefings. When classified briefings are prepared, the title (first) slide must display the same basic information as found on a document, and bear the highest classification of all information within the presentation. Each following slide must be marked with the classification level of the information on that particular slide. Should varying levels of classification be present on individual slides, those information pieces will be individually marked as if they were in a document.

3.2.7. Marking Magnetic Media. All approved magnetic media (floppy disks, hard drives, compact disks, video tapes, USB sticks, etc.,) will bear external markings clearly indicating classification, special handling instructions, control number, classification authority and downgrading instructions. Refer any questions or concerns to your unit SM.

3.2.8. Marking File Folders and Binders. File folders and binders containing classified documents will be conspicuously marked at the top and bottom, front and back, with the highest classification of any material contained therein. Coversheets may be used in lieu of markings on binders.

3.2.9. When applicable, copies of "Classified When Filled In" worksheets and databases are to be limited in distribution and collected/shredded by the exercise and/or class lead instructor.

3.3. Coversheets:

3.3.1. A coversheet must be attached to every document upon creation, receipt, or distribution of the document. Coversheets will consist of an overall classification centered at the top and bottom, subject, date, control number (Top Secret only), copy number, page number and distribution list. All classified documents being transported throughout the hallways or common areas must be contained in either a sealed envelope or a locked brief case. Refer to your unit SM for procedures and guidelines within your facility. NOTE: Classified information must never be printed on or attached to the outside of the protective envelope or brief case.

3.4. Working Papers:

3.4.1. Information that is being frequently changed or worked on during preparation of a finished document can be assigned "Working Paper" status. A Working Paper is marked with the words "WORKING PAPER" in the upper right-hand corner along with a "Destroy NLT" date. Additionally, working papers must identify the originator/date, appropriate classification.

3.4.2. Working papers are only good for 180 days after date of origin. After 180 days, they must be brought into formal accountability as a final document or destroyed. EXCEPTION: Working papers created during the planning phases of an exercise or experiment may be retained until completion of the applicable event.

3.4.3. Personnel may transmit properly marked working papers outside our 505 CCW channels during the 180-day retention period for official coordination and finalization. If received from an outside organization, working papers will be brought into accountability within 180 days of receipt.

3.4.4. "DRAFT" documents received from outside agencies will be considered Working Papers. The date of origin, if not marked on outside cover of document, will be considered the date the AF Form 310 or other applicable receipt document is signed. Once past the 180-day mark, document must be finalized or destroyed.

3.5. Security Containers:

3.5.1. The number of personnel knowledgeable of security container combinations and doors will be limited to appropriately cleared military, DoD civilian, contractor personnel and authorized visitors who have a valid need to know. All affected 505 CCW facility combinations must be changed and documented upon completion of the visit. The unit SM

will maintain a record of all combinations, the date each combination is changed, the names of individuals making the change and all safe custodian information.

3.5.2. The unit SM and/or appropriate safe custodian will ensure all combinations are changed according to the following schedule:

3.5.2.1. When combination lock is first installed or used, and at least annually thereafter.

3.5.2.2. When combination has been possibly or actually compromised.

3.5.2.3. When individuals possessing the combination PCS, PCA or have been placed in an "Unfavorable" Status.

3.5.2.4. Any other time considered necessary by CCs or SMs.

3.5.3. All combinations will be safeguarded in accordance with the highest classification of the material authorized for storage in the container.

3.5.4. Security containers will not be left open unless under constant surveillance of a 505 CCW member authorized access to all levels of information stored within the container.

3.5.5. A "clean desk" policy and use of the SF 701, End-of-Day Checklist, will be enforced in Open Storage areas and areas containing individual safes.

3.5.5.1. SF 701s will include a separate line item entry for an actual physical check of SIPRNET drop boxes located in work areas.

3.5.5.2. SF 702s, Security Container Check Sheet, will be used at each SIPRNET drop box.

3.5.6. Magnetic OPEN/CLOSED labels must be on all safes, SCIFS and SIPRNET drop box used by all Wing, Group, and squadron personnel.

3.5.7. All NATO (if applicable) classified will be kept separate from other classified information, in a separate drawer or container.

3.5.8. All TDY personnel must be briefed about Overnight Repository prior to transporting classified information. In the event an individual requires the use of the Overnight Repository, they must call the gaining base Command Post, receive instructions and ensure Command Post personnel have positive control of the classified materials and issue an AF Form 1297 as proof of exchange and custody of the material. Once complete, individuals will notify their local SM to update the status of the material(s).

3.6. Packaging Classified for Transport:

3.6.1. Specific requirements exist for packaging classified material for transport. The owners of the individual information or material are responsible for correctly packaging their classified for transport and delivery. Local SMs are trained to help individuals properly wrap classified packages and willing to assist in this process as needed.

3.6.2. Classified material will be double wrapped with an opaque covering. Exception: a locked briefcase, container or pouch may act as the second wrap for local couriers. Refer to your local SM or base supply for any questions concerning wrapping material for mailing classified via FEDEX.

3.6.2.1. The inner most wrapper will be conspicuously marked on all sides with the appropriate classification. The front of the inner wrapper will be annotated with a sequential package number (also annotated on receipt) and sender and recipient addresses. Address to a person or activity (organization) for information classified Top Secret/SCI and below.

3.6.2.2. The second or outer wrapper must be annotated with the complete address of the sender and recipient and the same package number applied to the inner wrapper and receipt. No person's name may be included on the outer wrapper.

3.6.2.3. Material must be wrapped with sufficient durability and strength to provide adequate protection against inadvertent opening/bursting during shipment. Flaps, corners and seams will be fully protected with reinforced tape.

3.7. Receipts:

3.7.1. Any transfer of classified material (courier or mail) will require a formal receipting action (except collateral classified Confidential). At a minimum, the receipt will provide complete identification of the material transferred and complete identification of all parties involved in the transfer. For courier and mail transfers, when a signed receipt is not returned within 30 days for CONUS or 45 days for OCONUS, immediately initiate tracer action. Reproduce a copy of the receipt held in suspense control files and mark it "TRACER - ORIGINAL RECEIPT NOT RECEIVED". Receipts will be maintained on file for 5 years.

3.8. Reproduction:

3.8.1. Security Managers will follow the established local security guidelines or policies to ensure all classified copiers are approved by the host base Security Forces prior to operation. Refer to your local SM for locations of authorized classified copiers.

3.9. Destruction:

3.9.1. 505 CCW personnel must continually review all classified holdings and reduce the quantity to the absolute minimum required to accomplish the mission. The organization is equipped with several National Security Agency-approved classified crosscut shredders and CD destroyers. Destruction procedures are as follows:

3.9.1.1. Destruction will be timely and conducted by appropriately accessed personnel. When possible, destroy classified material immediately after it has served its purpose, but not later than 30 days after being designated for destruction. The commander will designate a "classified holdings clean-out day" once a year (normally held in December) to ensure personnel are not retaining classified material longer than necessary.

3.9.1.2. Ensure all materials are completely destroyed and residue is unreadable and incapable of reconstruction/retrieval. Pending destruction, classified waste will be stored in an appropriate security container.

3.9.2. When destruction is deemed appropriate, tapes and floppy disks will be fed into a shredder. Removable hard drives will be disassembled and the platters removed and delivered to 505 TRG/SF for further disposition. All personnel are encouraged to deliver outdated classified compact disks (CDs) to your local SM for destruction.

3.9.3. A Certificate of Destruction will be accomplished whenever accountable and controlled material is destroyed. Two appropriately accessed individuals will accomplish and witness the destruction and sign the destruction certificate. Destruction certificates will be maintained on file for 5 years.

3.9.4. When applicable, COMSEC paper materials will be shredded to the 1 mm x 5 mm standard. All personnel should contact your local COMSEC representative or SM for assistance locating an appropriate shredder.

3.9.5. The Hurlburt Field Central Destruction Facility will be used to destroy large quantities of paper FOUO and classified information. Training is required prior to operation. Call 4-4729 to schedule an appointment for training.

3.10. Network and Computer Security:

3.10.1. Formerly known as Automated Information Systems security, this security discipline requires close interaction with 505 CS/SCXS, Information Assurance office.

3.10.2. Computer and networked systems used to capture, create, store, process or distribute classified and controlled unclassified information must be operated so that the information is

protected against unauthorized disclosure or modification. Protection requires a balanced approach that includes hardware/software protection features as well as administrative, operational, physical and personnel controls. Protection is commensurate with the classification level and category of the information being processed, and the threat and the operational requirements associated with the environment of the networks and connected computers.

3.11. Communications Security:

3.11.1. Telephones continue to be an area of security interest throughout the U.S. Government and industry. Government Intelligence agencies recognize foreign intelligence agencies operate numerous telephone intercept stations around the world to monitor telephone traffic on a daily basis. All personnel have been advised of this and are continuously cautioned in the use of telephones.

3.11.2. The primary authorized telephones for "secure" communications are STU-III, STE, and designated Voice of Internet Protocal (VoIP) instruments. However, each devices effectiveness is only as good as the individual operating it. All classified and/or sensitive information discussed over a STU-III, STE or VoIP phone must be done so in the "secure" mode.

3.11.3. Classified and/or sensitive information must not be discussed over an "open" (non-secure) line, or in the immediate surrounding area of an "open" line. Talking around or using gimmicks/codewords to emphasize a point are not authorized. Personnel will be cautioned that even though information standing alone may be unclassified, the compilation of various unclassified items may reveal classified or program-sensitive activities.

3.11.4. The STU-III or STE Responsible Officer is responsible for ensuring all STU-IIIs and STEs are in good working order and equipped with a valid Crypto Ignition Key (CIK) for the STU III and the Fortezza cards for the STEs.

3.12. Portable Electronic Devices:

3.12.1. Due to the wide availability of Portable Electronic Devices (PEDs), and their increasing functionality for storage, system connection, and transmission capabilities, they pose a distinct threat to 505 CCW networks. PEDs include but are not limited to PDAs, cell phones, laptop and handheld computers, thumb drives, and any other device or media capable of connecting to, recording, or transmitting voice, video, or network data.

3.12.2. Privately owned PEDs are not allowed within any classified working area. This includes offices having SIPRNET drop boxes that are open and actively being used. The user of the SIPRNET drop box is responsible for alerting personnel within the working area that the SIPRNET network is now active, and all PEDs must be removed. Individuals having a mission requirement to use government or approved corporate-owned PED on a classified network will have the device authorized through 505 CS/SCXS, Information

Assurance office and 505 TRG/SF Wing Security office via the Media Exception Letter located in SharePoint https://ccw.hurlburt.af.mil/sites/505TRG/Security/default.aspx Shared Documents/General Security Forms/Media Exception Letter. Subordinate units are encouraged to adopt local procedures that build upon this requirement to curtail the unauthorized use of PEDs in their respective classified working areas.

3.12.2.1. The Information Assurance office is the initiating approval authority for the Media Exception Letter. The original Media Exception Letter will accompany the approved PED, the wing security office will maintain a copy for a period of one year.

3.12.3. Privately-owned PEDs must be virus scanned by the Information Assurance office prior to connecting to an unclassified AF network, including floppy disks, CDs, DVDs, thumb drives, external hard drives, etc.

Chapter 4

INDUSTRIAL SECURITY

4.1. General:

4.1.1. The 505 CCW Industrial Security Program will be administered IAW DoD, AF, ACC and host base/local guidance. Because of our status as a geographically separated wing with units and detachments serving as ACC tenant units on host installations, the flow of contractual documents, clearance verification, visit requests and classified access requests are different than those outlined in DoD and AF guidance. Non-Hurlburt units will use host-base industrial security resources available through their local SF office.

4.2. ACC Requirements:

4.2.1. HQ ACC/INS (SSO) has oversight authority over 505 CCW contracts performed at Hurlburt Field that require SCI access for contract performance. AFSOC/SSO has collateral security authority over these same contracts.

4.2.1.1. The responsible program/project officer will prepare new DD FM 254, Contract Security Classification Specification, with the assistance of the wing security office. Draft DD FM 254 will be routed through HQ ACC/SSO for coordination/approval prior to access to SCI information by contractors working against that contract number.

4.2.1.2. The servicing SSO of the organization providing funding and SCI materials controls SCI access for the new contracts. New DD FM 254s will be coordinated through that servicing SSO.

4.2.1.3 Section 10 of the DD FM 254 will dictate the coordination flow for the form. The ACC OPR for each access requirement outlined in Section 10 will validate that DD FM 254 (i.e., COMSEC, Restricted Data, etc.).

4.2.1.4. Once validated by the ACC OPRs, the DD FM 254 will be routed through host base installation OPRs for items marked yes in section 10 of the form.

4.2.1.5. When a DD FM 254 is approaching expiration; contact the program/project officer to determine if a new DD FM 254 has been initiated, or if contract options have been exercised via Standard Form 30, Amendment of Solicitation/Modification of Contract.

4.2.1.6. An AF FM 2587, Security Termination Statement, is required for all contractors no longer working in the 505 CCW facilities. This is accomplished by the SM or designee and will be part of a contractor inprocess/outprocess checklist. It will be maintained on file for a period of 2 years. HQ ACC/INS will be notified

when a contractor retires or terminates employment on contracts worked in 505 CCW facilities.

Chapter 5

PHYSICAL SECURITY

5.1. General:

5.1.1. All 505 CCW personnel have a responsibility to ensure security of our facilities. Although force protection conditions are in place, personnel should remain vigilant and alert to changing security conditions. Complacency has no place in an environment handling, processing and storing classified information and materials.

5.2. Entry and Access Control:

5.2.1. Once issued, individuals are responsible to protect the badge and the code allowing facility entry. Individuals who have not had their security clearance verified by a 505 CCW/ SM or an authorized Mission Support Element (MSE) (during large-scale exercises or experiments) aren't authorized access to classified information or materials. All uncleared personnel or visitors will be issued an escort badge denoting "unclear" and not authorized within a classified area without a cleared and trained escort official. Refer to your local SM for further assistance on escort information.

5.2.2. All personnel assigned to the 505 CCW have the following responsibilities:

5.2.2.1. Challenge and assist any individual(s) not recognized as having unescorted access into the facility.

5.2.2.2. Be sufficiently aware of the surroundings in the facility so as to detect any possible compromise, whether inadvertent or intentional. This may include but is not limited to:

5.2.2.2.1. Physical changes in a workspace without apparent reason.

5.2.2.2.2. Any indication of forced or surreptitious entry to the facility.

5.2.2.2.3. Unexplained presence or inappropriate absence of a co-worker.

5.2.2.2.4. Other undue curiosities toward 505 CCW activities or materials by anyone.

5.2.2.3. An occurrence of any situation described above must be immediately reported to your local SM, designated alternate, OSI or host base SFS.

5.2.3. All visitors must be cleared to access classified information. This not only means contractors and visitors, but students and other government personnel. The SM must verify clearance information prior to the individual being granted access. Approved forms of verification include: Joint Personnel Adjudication System (JPAS) verification, an official Visit Request from the parent organization, or faxed verification from the individual's unit/company SM or SSO.

5.2.3.1. Visitors will not access SCI information at any 505 CCW unit unless a valid visit certification is passed from the visitor's servicing SSO to the host-base SSO. Again, this is the only authorized means of accepting and verifying a visitor's access to SCI.

5.2.3.2. Security managers with internal door combinations (such as cipher locks when activated) should exercise extreme caution when distributing combinations to non-permanent party personnel. All door combinations will be changed as required immediately upon completion of the event by the SM or building custodian.

5.3. Network and Classified Working Area Defense:

5.3.1. IAW DoD AI 26, para 5-205.2.2.11, electronic or optical devices are prohibited from classified portions of briefings, instruction or meetings conducted throughout the 505 CCW. The commander, along with the security staff, has final decisive authority regarding introduction of electronic devices into classified working areas.

5.3.2. Unless approved by the Information System Security Officer (ISSO) and unit security manager, the following items are prohibited across the 505 CCW while operating within classified working areas or classified functions:

CELLULAR CAMERA/PHONES
TWO-WAY PAGERS
CAMERAS
EXTERNAL CD/R/RW, DVD/R/RW, FLOPPY OR HARD DRIVE UNITS
USB FLASH HARD DRIVES
LAPTOP PCs
PDAs
USB MEMORY STICKS OR HARD DRIVES
RECORDABLE WATCHES AND WATCH CAMERAS

5.3.3. At no time may any personally owned device be attached to 505 CCW classified/unclassified system architecture without the written permission of the local 505 CCW SM, Client Support Administrators (CSA), lab manager or commander. A 505 CCW Media/Electronics Exception letter (see Attachment 1) will be completed to authorize the electronics/media into the classified working area. Mediation Letter can be found at https://ccw.hurlburt.af.mil/sites/505TRG/Security/default.aspx under the Shared Documents/

General Security Forms/Media Exception Letter. Willfully connecting personal devices to these networks without proper permission is considered subversive activity and may be punishable under the Article 15 of the UCMJ and other federal law.

5.3.4. Personal software other than that required to support event initiatives is prohibited from being loaded onto 505 CCW computers.

5.3.5. Blank media, including CD/R/RW, DVD/R/RW, JAZ, ZIP, floppy disk, mini-disk or magnetic tapes are expressly prohibited. Music CDs are not permitted in classified work areas without a risk-management determination by your local 505 CCW SM, given the inability to discern original factory CDs from CD/R/RW with aftermarket labels applied. Music on recordable media is not authorized under any circumstances. All authorized recordable media must be marked IAW DoD standards, according to its classification. Unmarked media in classified working areas will be immediately marked and labeled or confiscated and destroyed.

5.4. Conducting Classified Briefings in Wing Conference Rooms (Hurlburt Field only):

5.4.1. Ensure personal electronics and media that are allowed into classified working areas are authorized via the Event Media/Electronics Exception Letter located in Attachment 1 of this document, also found on the "Y" drive under Security Forms. The unit SM will sign this letter to ensure proper risk determination has been made regarding the electronics or media in question.

5.5. End-of-Day Security Checks:

5.5.1. Regardless of the length of time 505 CCW offices are open, an end-of-day security check must be conducted before each facility containing a classified storage container or open storage area, is secured. Each end-of-day security check must be performed and documented on the SF 701. (https://ccw.hurlburt.af.mil/sites/505TRG/Security/default.aspx under the Shared Documents/General Security Forms/SF701). Specific procedures are as follows:

5.5.1.1. All 505 CCW personnel are responsible for ensuring their respective work areas are free of classified materials and unclassified but sensitive materials are locked away. The 505 CCW/CC has mandated a "clean desk" policy in an effort to prevent inadvertent access to classified materials by unauthorized individuals.

5.5.1.2. The SF 701 contains a list of items that must be checked each day. The last individual out of the office will physically check each item listed on the form, then place their initials and time checked in the appropriate blocks.

5.5.1.3. The last individual will also annotate the SF 702, Security Container Check Sheet, SF 702 located (https://ccw.hurlburt.af.mil/sites/505TRG/Security/default.aspx

under the Shared Documents/General Security Forms/702) for every security container opened during the day. The security container will be checked to ensure it is actually closed by spinning the dial clockwise and attempting to turn the handle. The individual will place their initials and the time the security container was checked. In the event the container was not opened that day, the individual will annotate the check sheet as such.

5.6. Emergency Action Plan (EAP):

5.6.1. Unit SMs will develop and maintain an EAP outlining responsibilities and general procedures for their respective personnel concerning the safeguarding of classified information during an emergency situation.

5.6.2. The EAP addresses procedures related to the loss of essential utilities, fire protection, natural disasters, sabotage, riots, civil disorders, and hostage or terrorist attack or capture. The EAP also includes evacuation procedures.

5.6.3. All assigned personnel should be familiar with their local EAP. They may be acquired by contacting your local SM for information and/or instructions.

5.6.4. SMs will review the EAP annually and update as necessary.

5.7. Physical Security Sweeps:

5.7.1. Unit security managers should conduct a quarterly after-hours physical security sweep of their facilities for lighting deficiencies and security issues. The Wing Security office will assist as required. The 1SOSFS Law Enforcement Desk will be notified at 884-7114 prior to initiating these sweeps to prevent overlapping any of their required facility checks.

5.7.2. Unit security managers will scan all work areas for logins and passwords, anti-robbery issues, lighting, etc., to give the responsible unit commander or his designee a picture of overall physical security of his facilities and systems.

5.8 SIPRNET Access:

5.8.1. SIPRNET access is granted to individuals possessing an appropriate security clearance of Secret or above. Contact your unit SM for instructions on acquiring SIPRNET accounts at your location.

Chapter 6

OPERATIONS SECURITY (OPSEC)

6.1. OPSEC Officer and Alternate:

6.1.1. Each unit commander will appoint a squadron OPSEC officer and alternate in writing. A SM should not assume this position. However, an operations officer or individual with the overall view and understanding of the complete unit operational mission is normally a better choice. The appointment letter (copy) will be forwarded to the local Information Operation Office and 505 TRG/SF.

6.2. OPSEC Procedures:

6.2.1. 505 CCW unit OPSEC officers will ensure OPSEC issues and information are distributed throughout the wing. Hurlburt units refer to 1SOW/IO at 884-4565 for additional information; all other units and detachments refer to host-base OPSEC offices.

6.2.2. Unit OPSEC officers will canvass subject matter experts within their organization to develop and maintain a critical information list for each unit.

Chapter 7

SECURE FACILITY PROCEDURES FOR BUILDING 90005 HURLBURT FIELD, FLORIDA

7.1. Authorized Personnel and General Information:

7.1.1. All personnel entering building 90005 must comply with established 505 CCW security rules, guidelines and procedures. All personnel must wear, in plain view, a 505 CCW issued security badge to gain access to any classified processing areas, meeting, conference, exercise or event. For those individuals who have not had their security clearance verified and issued a cleared security badge, they will fall into the uncleared visitor category. All uncleared visitors will be issued a red badge (or no badge) indicating the individual is not authorized access to any classified information or material. Locally electronic databases are authorized and can be maintained in the unit SM office. Authorized personnel within the building should challenge any unauthorized person who enters this building while hosting a classified event, meeting, or conference and immediately notify 505 TRG/SF for security verification.

7.1.2. Building 90005 will have a military or government civilian representative present during classified meetings, conferences, or while events are in session and any time classified processing is being performed. This representative's duties include ensuring security procedures are followed, such as addressing and correcting problems and ensuring

all classified information and materials are properly safeguarded and stored when not in use. 505 TRG/SF or the responsible security manager must be notified immediately of any security deviation resulting from compromise or procedure shortfall.

7.2. Classified Magnetic Media in Building 90005:

7.2.1. Visitors will not introduce recordable media into 505 CCW classified working areas, unless approved through proper channels before event. If media is required for accomplishment of the event, it will be given to the event lead and scanned for viruses/malicious software prior to introduction into wing network architecture by the 505 CS/SCXS Office for approval. It will be conspicuously marked to the classification level of the material it contains or system it is utilized on.

7.2.2. Government or authorized corporate owned electronics or media deemed necessary for exercises, events, or conferences will be processed through 505 CCW/IA, Information Assurance, and the Wing Security office. This will be accomplished on the Event Media /Electronics Exception Letter (Attachment 1) reference 3.12.2 of this OI. The Information Assurance office will sign off first to ensure the electronics or media have been virus and compatibility-tested.

7.2.3. Visiting personnel will surrender all media to event leads or node chiefs at the end of their duty day. In addition, event leads or node chiefs will ensure a check is made for classified disks, drives or papers in the secure working area prior to departing and ensure all materials are properly stored in available security containers. Computers and classified disks in operation overnight may be left unattended, if the facility is approved for open storage (i.e., computer room, mezzanine or bay floor when assigned a security detail).

7.2.4. Event leads are responsible for ensuring all classified material and classified output (printed paper, printer toner/ribbons, floppy disks) have been accounted for and properly inventoried at the end of each event. At the conclusion of each event involving classified material, a 505 TRG/SF representative must make a "final sweep" of the area to deem the area "all clear."

7.3. Processing Classified:

7.3.1. A local SM or Event Host representative will brief local security procedures to visiting personnel prior to any classified briefing, meeting or conference being conducted within 505 CCW facilities. This briefing must cover at a minimum, badge operations, proper safeguarding of classified information, local safety briefing and POCs for after-hours contact.

7.3.2. During on-going operations with the classified system, no unauthorized personnel will be admitted past access/entry control points without being properly escorted. Visitors

must enter and exit the facilities only through the access/entry control point. Only in cases of emergencies will other exits be authorized for use.

7.3.3. At no time will a printer or other output media (i.e., tape drives or floppies) be connected to the classified systems without approval from the local SM or CSA. If it becomes necessary to connect such devices, output products should be properly accredited, marked and handled IAW DoD, Air Force, and 505 CCW instruction.

7.3.4. The 505 CCW host or representative will ensure all areas are secured and end-of-day checklists are signed prior to departing.

EDWARD L. McKINZIE, Colonel, USAF
Commander, 505th Command and Control Wing

Attachment 1

EVENT MEDIA/ELECTRONICS EXCEPTION LETTER

MEMORANDUM FOR ALL PERSONNEL

FROM: 505 CCW/CC

SUBJECT: Event Media/Electronics Exception Letter _____
(EVENT)

1. IAW 505 CCW Instruction 31-2, the listed media and/or electronics are authorized transport into and out of classified working areas during _____, by the following individual:

NAME	RANK	CONTACT NUMBER	SSAN

DESCRIPTION	QUANTITY	SERIAL NUMBER	REMARKS

2. This letter must accompany the listed materials at all times, and is not valid without the signature of the Information Systems Security Officer (ISSO) or designee, and a security manager. Include valid dates in the remarks column. Contact the event project officer or security officer with any questions.

_____ _____
505 CCW/ISSO 505 CCW/SF Signature

_____ _____