BY ORDER OF THE COMMANDER,
18TH WING (PACAF)

18TH WING INSTRUCTION 33-202

13 MAY 2002

Communications

WING COMPUSEC PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: 18 CS/SCBS (MSgt Bryan W. Smith)

Certified by: 18 SPTG/CC
(Col Thomas F. Berardinelli)
Pages: 10
Distribution: F

This instruction provides direction for the implementation of a base-wide COMPUSEC program at Kadena AB, Okinawa. It implements AFPD 33-2, *Information Protection*. It contains specific procedures, augmenting Air Force Instruction 33-202, *Computer Security*, to effectively establish the local COMPUSEC Program and applies to all personnel assigned, attached or OPCON to the 18th Wing (contractors, civilians, civil service and all military services) either temporary or permanently from any agency. It also applies to all proposed or existing Information Systems (IS), networks, and resources, such as computers, remote terminals, peripherals, applications/systems software, contractual services, and facilities under the control of or attached to the 18th Wing. It applies to 18th Wing and associate units at Kadena AB. This publication also applies to the Air National Guard or US Air Force Reserve.

1. General.

1.1. Program Objectives.

1.1.1. The COMPUSEC program is designed to enable personnel to reach the following base goals:

1.1.1.1. To ensure a recognizable, comprehensive COMPUSEC program.

1.1.1.2. To ensure the availability, integrity, and confidentiality of IS resources and processed information throughout an IS' life cycle.

1.1.1.3. To ensure the maximum level of protection against threat and vulnerability to avoid denial of service, corruption, compromise, and Fraud, Waste, and Abuse (FWA).

1.1.1.4. To ensure COMPUSEC education and guidance are provided to all IS users and managers.

1.1.1.5. To develop and implement procedures and polices to prevent violations and security deviations or incidents.

1.2. Program Administration.

1.2.1. The Kadena COMPUSEC program will be administered at two levels:

1.2.1.1. Wing Level:

1.2.1.1.1. The Wing Information Assurance Office will be responsible for providing general guidance, establishing and publishing base COMPUSEC policy, inspecting units for COMPUSEC compliance and monitoring of the base Certification and Accreditation (C&A) process.

1.2.1.2. Organization Level:

1.2.1.2.1. Base organizations will be responsible for compliance with published COMPUSEC policy and implementation of COMPUSEC programs.

2. Responsibilities.

2.1. Wing Information Assurance Office.

2.1.1. Develop and maintain a formal base-wide IS security program.

2.1.2. Issue COMPUSEC policies and inspect for compliance.

2.1.3. Provide COMPUSEC and Information Assurance (IA) guidance to base IS users.

2.1.4. Maintain a Wing IA web page.

2.1.5. Maintain 7-part folders on organizations in accordance with AFI 33-202, *Computer Security*.

2.1.6. Maintain a tracking system of organization Foreign National Request of Access packages.

2.1.7. Maintain a file of each organization's Foreign National Request for Access package.

2.1.8. Forward Foreign National Request for Access packages to the Wing Commander for review and signature.

2.1.9. Inform UCMs and Network Control Center (NCC) of foreign national access approval/disapproval.

2.1.10. Provide guidance to Unit COMPUSEC Managers (UCMs) in drafting IS C&A packages.

2.1.11. Review and endorse (when applicable) completed C&A packages.

2.1.12. Forward C&A packages to the Designated Approving Authority (DAA) for approval.

2.1.13. Maintain a repository of completed C&A packages.

2.1.14. Maintain a tracking system to ensure base-wide compliance with C&A requirements.

2.1.15. Provide C&A metrics to MAJCOM as required.

2.1.16. Maintain copies of all Unit COMPUSEC Manager (UCM) appointment letters.

2.1.17. Conduct initial UCM training on a quarterly basis.

2.1.18. Assist UCMs in development of unit COMPUSEC programs.

2.1.19. Develop, publish, and disseminate COMPUSEC policies and procedures.

2.1.20. Conduct weekly no-notice UCM inspections.

2.1.21. Maintain copies of all Information Assurance Awareness Program (IAAP) Manager appointment letters.

2.1.22. Conduct initial IAAP Manager training on a quarterly basis.

2.1.23. Create and disseminate IA products to IAAP Managers on a bi-weekly basis.

2.1.24. Conduct weekly no-notice IAAP Manager inspections.

2.1.25. Task IAAP Managers to conduct annual IA assessments.

2.1.26. Conduct quarterly Telecommunications Monitoring Assessment Program (TMAP) surveys.

2.1.27. Prepare bi-annual TMAP report for MAJCOM.

2.1.28. Maintain base-level TMAP certification.

2.1.29. Maintain a tracking system of UCM inspections.

2.1.30. Maintain a tracking system of IAAP Manager inspections.

2.2. Unit COMPUSEC Managers (UCM): Will be appointed in writing by the unit Commander. UCMs must be either active duty military or US DoD civilian.

2.2.1. Provide a copy of the appointment letter to the Wing IA Office.

2.2.2. Devise and implement a unit COMPUSEC program that complies with this Operating Instruction, all base COMPUSEC policies (listed on **https://www.kadena.af.mil/wiao**), AFI 33-202, AFI 33-202/PACAF Supplement 1, *Computer Security*, AFMAN 33-229, *Controlled Access Program*, AFMAN 33-203, *Emission Security*, AFSSI 5020, *Remanence Security*, AFSSI 5021, *Vulnerability and Incident Reporting*, and DOD 8510.1-M, *Department of Defense Information Technology Security Certification and Accreditation Process*.

2.2.3. Act as the SINGLE liaison between the unit and the Wing IA office for all computer and network security matters.

2.2.4. Ensure visual aids are posted throughout the unit informing users who their UCM is and that the UCM should be contacted if they have COMPUSEC questions/concerns.

2.2.5. Develop and implement a program to ensure unit compliance with computer or network security taskings passed down from Wing Information Assurance, Information Protection Office or NCC (typically PACAF initiated Notice To Airmen [NOTAM], Time Compliance Network Order [TCNO] and Communications Tasking Order [CTO] directives). Report compliance as directed, normally through the Help Desk. Tracking metrics should be included in 7-part COMPUSEC/EMSEC Folder.

2.2.6. Ensure unit Functional System Administrators (FSA) and Work Group Managers (WGM) control access to files, software and devices so that only authorized users have access.

2.2.7. Ensure unit FSAs and WGMs provide each user with only those system privileges needed for assigned tasks (least privileged concept).

2.2.8. Ensure unit FSAs and WGMs limit access to privileged programs, utilities, and security-relevant programs/data files.

2.2.9. Ensure unit FSAs and WGMs limit the capability to conduct privileged actions (loading new users, password management, patching system files etc) to authorized personnel.

2.2.10. Ensure unit FSAs and WGMs implement C2 auditing on servers in accordance with AFMAN 33-229.

2.2.11. Ensure FSAs and WGMs have passwords that are 12 characters minimum, and contain upper and lower case alpha characters, at least 1 number and at least 1 special character.

2.2.12. Ensure FSAs and WGMs are familiar with the contents of KBAN and SKBAN Policy and Procedures guides.

2.2.13. Ensure all group accounts are approved by the DAA and Group Account Sign-In logs are maintained and filed (see 7-part COMPUSEC/EMSEC folder).

2.2.14. Ensure unit software licensing compliance. All software should be licensed either through the base Enterprise Software License Policy or unit purchases. Licensing documentation and information should be filed in 7-part COMPUSEC/EMSEC folder.

2.2.15. Ensure all users utilize screen savers that are password protected.

2.2.16. Ensure unit personnel follow correct procedures and report events that affect the security of an IS (classified message incident, virus, hacker or theft).

2.2.17. Implement and maintain the Foreign National Request for Access program within your unit. Ensure packages are filed (see 7-part COMPUSEC/EMSEC folder).

2.2.18. Report all security violations and incidents to the Wing IA office.

2.2.19. Ensure users appropriately label all classified media (Standard Form 711, **Data Descriptor**, and classification sticker).

2.2.20. Ensure users appropriately destroy all classified media.

2.2.21. Know the location of all servers within your unit.

2.2.22. Ensure C&A is obtained on all IS within the unit before they are operational. Ensure a process is developed with the unit ADPE Custodian to facilitate this requirement. Make FSAs and WGMs are of this requirement.

2.2.23. Ensure C&A is reaccomplished as required (KBAN/SKBAN appendixes should be updated every quarter - independent networked systems [no KBAN/SKBAN connectivity] and standalones every three years - or when significant changes are made that impact security).

2.2.24. Designate a Certifier during the initial phases of the C&A process.

2.2.25. Submit C&A documents to the Wing IA office for review.

2.2.26. Maintain a file of all C&A information for your unit (see 7-part COMPUSEC/EMSEC folder).

2.2.27. Ensure controls are in place for the removal of user accounts when no longer necessary.

2.2.28. Ensure virus protection software is installed on all IS (including stand-alones and laptops) within the unit and the latest virus signature files are loaded.

2.2.29. Ensure the “consent to monitoring and warning” notice runs on all IS (including stand-alones and laptops) during boot up/logon.

2.2.30. Ensure users disable ActiveX and Java features in Internet Explorer when visiting non-.gov or .mil sites.

2.2.31. Ensure users with Personal Data Assistants (PDA) conform to base PDA policy.

2.2.32. Ensure users accessing the Kadena Base Area Network (KBAN) utilizing remote access via Asymmetric Digital Subscriber Line (ADSL) modem conform to base ADSL Modem Policy.

2.2.33. Ensure IS with KBAN connectivity have connectivity to KBAN only - i.e. no modem connectivity to another system.

2.2.34. Ensure there are current EMSEC certification letters on file for all classified systems (see 7-part COMPUSEC/EMSEC folder).

2.2.35. Request the Wing IA office conduct an EMSEC assessment on all new classified systems before they become operational.

2.2.36. Implement and maintain countermeasures required or deficiencies identified as a result of any EMSEC assessment.

2.2.37. Initiate requests for temporary and permanent waivers and EMSEC tests when required per AFI 33-203, *Emission Security Program*.

2.2.38. Ensure RED equipment is separated from BLACK signal lines by 20 inches.

2.2.39. Ensure no telephone instruments touch RED equipment.

2.2.40. Ensure every signal line from RED equipment is routed through only other RED equipment or encrypted before connection to BLACK equipment.

2.2.41. Ensure RED signal lines are separate from BLACK signal lines by a distance sufficient enough to easily distinguish each line.

2.2.42. Ensure all RED signal lines are marked with a 1-inch wide strip of red tape or red paint at intervals of approximately 1-1/2 meters.

2.2.43. Ensure RED equipment is separated from BLACK tape players or recorders, video recorders and unclassified data recorders or players by 10 meters.

2.2.44. Maintain a 7-part COMPUSEC/EMSEC folder as follows:

2.2.44.1. Part 1 - Identification and Training.

2.2.44.1.1. Unit UCM Appointment Letter.

2.2.44.1.2. List of unit Information System Security Officers (ISSO) and/or Terminal Area Security Officers (TASO).

2.2.44.2. Part 2 – Policy.

2.2.44.2.1. Copy of this Operating Instruction.

2.2.44.2.2. KBAN/SKBAN Policy and Procedures.

2.2.44.2.3. COMPUSEC Policy Letters.

2.2.44.2.4. All C&A information for IS in your unit (may be cross referenced to another location).

2.2.44.2.5. ADPE listing of all IS in the unit (may be cross referenced to another location - each entry must have cross reference to specific C&A paperwork).

2.2.44.3. Part 3 – Metrics.

2.2.44.3.1. NOTAM, TCNO and CTO suspense compliance tracking (may be cross referenced to another location).

2.2.44.3.2. Any metrics provided to Wing IA office.

2.2.44.4. Part 4 - EMSEC and Security Incidents.

2.2.44.4.1. EMSEC certification letters (for classified systems).

2.2.44.4.2. Any security incident reports.

2.2.44.5. Part 5 - Correspondence.

2.2.44.5.1. Group Account requests.

2.2.44.5.2. Completed Group Sign-In Logs.

2.2.44.5.3. Foreign National Account Request packages (may be cross referenced to another location).

2.2.44.5.4. Software licensing documentation.

2.2.44.5.5. PDA Letters of Understanding.

2.2.44.5.6. Modem Waivers.

2.2.44.5.7. General correspondence.

2.2.44.6. Part 6 - Self Inspections.

2.2.44.6.1. Copy of last unit COMPUSEC inspection.

2.2.44.6.2. Copy of any self-assessments conducted.

2.3. IAAP Manager: Will be appointed in writing by your unit Commander.

2.3.1. Devise and implement a unit IAAP program that supports the Wing IA program. Ensure the program complies with this Operating Instruction and AFI 33-204.

2.3.2. Disseminate IA materials received from the Wing IA office and display awareness aids throughout the organization.

2.3.3. Ensure users are familiar with Air Force software licensing, software management and anti-piracy policies as contained in AFI 33-114, *Software Management*.

2.3.4. Ensure all users complete the Licensing Network Users CBT before being allowed to access the network and the completion certificates are filed.

2.4. ISSO: ISSOs are responsible for: 1) administering the security requirements for an IS during its operation 2) monitoring the secure operation of an IS within the environment defined in the SSAA. ISSOs are designated by the UCM - logical choices for ISSOs would be WGMs and FSAs. If ISSO positions are not assigned, these responsibilities reside with the UCM.

2.4.1. Establish controls to ensure users operate, maintain and dispose of IS according to existing policy and procedure.

2.4.2. Ensure the system security plan for each IS is distributed to system users.

2.4.3. Establish controls that ensure audit trails are periodically reviewed.

2.4.4. Perform initial evaluation of discovered vulnerabilities or incidents and begin corrective or protective measures and reporting in accordance with AFSSI 5021.

2.4.5. Evaluate known vulnerabilities to ascertain if additional safeguards are needed to protect IS.

2.4.6. Take aggressive action to implement and report compliance with TCNO and CTO taskings.

2.4.7. Periodically validate user-access privilege levels.

2.4.8. Ensure the system operates within constraints of the system and network security policies.

2.4.9. Ensure only software approved by the DAA resides on the system.

2.4.10. Continually identify threats, deficiencies and associated countermeasures.

2.4.11. Establish restrictions on shared usage of programs or files.

JEFFREY A. REMINGTON, Brigadier General, USAF
Commander, 18th Wing

Attachment 1

GLOSSARY OF REFEREMCES AND SUPPORTING INFORMATION

Abbreviations and Acronyms

AFI—Air Force Instruction

AFSSI—Air Force Systems Security Instruction

AFMAN—Air Force Manual

C&A—Certification and Accreditation

C2—Criteria class outlined in DoD 5200.28-STD

CBT—Computer Based Training

COMPUSEC—Computer Security

CSM—Computer Systems Manager

CSSO—Computer Systems Security Officer

CTO—Communications Tasking Order

DAA—Designated Approving Authority

DoD—Department of Defense

EMSEC—Emission Security

FSA—Functional System Administrator

FWA—Fraud, Waste and Abuse

IA—Information Assurance

IAAP—Information Assurance Awareness Program

IPO—Information Protection Office

IS—Information System

ISSO—Information System Security Officer

KBAN—Kadena Base Area Network

MAJCOM—Major Command

NCC—Network Control Center

NOTAM—Notice To Airmen

PDA—Personal Data Assistant

PACAF—Pacific Air Forces

SSAA—System Security Authorization Agreement

TCNO—Time Compliance Network Order

TASO—Terminal Area Security Officer

UCM—Unit COMPUSEC Manager

WGM—Work Group Manager

Terms

Accreditation—Formal declaration by the DAA that an IS is approved to operate in a particular security mode using a prescribed set of safeguards and controls.

Certification—Comprehensive evaluation of the technical and non-technical security features, and countermeasures of an IS to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certifier—Individual responsible for making a technical judgment of the IS's compliance with stated security requirements and requesting approval to operate from the DAA.

Controls—Prescribed actions taken to maintain the appropriate level of protection for ISs. Controls may validate security activities, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of AIS activities or report incidents. **NOTE:** There are two divisions of control: management (policy, objectives, and criteria class) and internal (security requirements, mechanisms, and rules).

Countermeasure—The sum of a safeguard and its associated controls.

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating an IS or network within a specified environment. On Kadena, this is the Wing Commander.

Information—Data derived from observing phenomena and the instructions required to convert that data into meaningful information. **NOTE:** Includes operating system information such as system parameter settings, password files, audit data, etc.

Information System—Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes software, firmware, and hardware. **NOTE:** The term "IS" includes stand-alone systems, communications systems, and computer network systems of all sizes, whether digital, analog, or hybrid; associated peripheral devices and software; process control computers; security components; embedded computer systems; communications switching computers; personal computers; workstations; microcomputers; intelligent terminals; word processors; automated data processing (ADP) systems; office automation systems; application and operating system software; firmware; and other IS technologies, as developed.

Information Systems Security Officer (ISSO)—Official who manages the COMPUSEC program for an IS assigned to them by the UCM; including monitoring IS activities and ensuring that the IS is operated, maintained, and disposed of according to security policies and practices.

Level of Protection—Established safeguards with controls to counter threats and vulnerabilities based on the security requirements. Assures availability, integrity, and confidentiality of the IS.

Safeguards—Protective measures and controls prescribed to meet the security requirements of an IS. **NOTE:** Safeguards include security features and management constraints from the various security disciplines (i.e., administrative, procedural, physical, personnel, communications, emanations, and computer security), used in concert to provide the requisite level-of-protection.

Threat—Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, or Fraud, Waste, and Abuse to a system.

Vulnerability—Defense weakness to control a threat to the IS.