7r/IN/32

System Security Authorization Agreement (SSAA)

for the

WIRE Archive and Research Facility

Room 2A103, Fairchild Hall

Department of Physics

United States Air Force Academy

12 Feb 2002

1.0 MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

1.1 System name and identification. The Wide-Field Infrared Explorer (WIRE) Archive and Research Facility (WARF) is operated and maintained by the Department of Physics, USAF Academy. The lab is located in Fairchild Hall, 2354 Fairchild Dr., Suite 2A103, USAF Academy, CO 80840. The WARF will be used for research and education in support of the NASA Wide Field Infrared Explorer (WIRE) satellite, and for related high-precision photometry missions and activities. The WARF will also contain the WIRE preliminary and final archives prior to their delivery to the National Space Science Data Center (NSSDC).

1.2 System description. The WARF consists of a suite of equipment purchased under several NASA grants in support of WIRE research. The core system consists of a Red Hat Linux workstation with twin 933 MHz PIII processors, 1 GB of RAM, 133 GB of hard disk space, and DAT and DLT tape drives. The WARF is also supported by several additional networked Linux workstations. Only one of these (an older 450 Mhz PIII computer running Red Hat Linux) is currently running, but the addition of several more is expected over the next year. In addition, a printer will soon be added.

The WARF will serve as the primary research facility for the analysis and archiving of data from the WIRE satellite, together with limited quantities of other high-precision astronomical photometry data from both ground- and space-based facilities. However, the archive to be created here will not be the final archive; rather, the archive will be duplicated at the NSSDC and public access to the data will generally take place through that site.

1.3 FUNCTIONAL DESCRIPTION.

1.3.1 System capabilities. The WARF will serve two primary purposes. The first is to serve as a site for the construction of the WIRE final archive, and for the development of data processing pipeline and analysis software for that purpose. The second purpose is to support science analysis of WIRE data. In support of these activities, certain services must be provided by the network, i.e. FTP, Telnet, DNS, print sharing, file sharing, and WWW services.

1.3.2 System criticality. The system will be used for educational and research purposes only. This system is not critical to the USAFA mission.

1.3.3 Classification and sensitivity of data processed. WARF is an unclassified system. It will be used for educational and research purposes only. No type of data requiring special handling (i.e. Privacy Act, financial, etc) is expected to be processed within the facility.

1.3.4 System user description and clearance levels. WARF will be used by the faculty and staff of the Department of Physics, Physics majors and minors, contractors working for DFP, and any other faculty, staff, or cadet of USAFA that requests access. On occasion, users from the university and NASA communities will retrieve or deposit data from public directories on the WARF, but such users will not run software on the system. The WARF is an unclassified system, so no special clearance levels are required.

1.3.5 Life-cycle of the system. The WARF is expected to be an integral part of the astronomy research program here at the Academy for several years to come. Currently, support is provided from NASA through FY 2004. The hardware and software within the lab will be upgraded and replaced on an as needed basis by DFP.

1.3 System CONOPS summary. The purpose of the system is to support WIRE data reduction and analysis, and the construction of a WIRE archive. When functioning in its data reduction/analysis mode, the system will essentially act as does any workstation, so details will not be presented here. At present, approximately half of the WIRE dataset resides at NASA Jet Propulsion Laboratory, but all data will be consolidated at USAFA during the first stage of operations. After that point, archive construction will begin through the creation of a set of unified software tools to act as a coherent and consistent pipeline for data reduction. During this time, both raw and reduced data will be shared with members of the broader astronomical community (i.e., outside USAFA) in order to develop a standard data reduction package which is acceptable to all users. Once this process is complete, the focus of effort will shift to applying the data reduction pipeline to all existing data, indexing the data, and finally delivering it to the National Space Science Data Center. More details are available in the (accepted) proposal to NASA which describes this process (see attachment).

2.0 ENVIRONMENT DESCRIPTION

2.1 Operating environment. The WARF is located in Room 2A103 of Fairchild Hall. This room is a departmental office within DFP. Accordingly, entry into DFP is controlled by a cypherlock. Only DFP personnel have access to this room. Subordinate workstations will be located in 2B19, an existing DFP laboratory, and the USAFA observatory. Entry to these rooms is controlled by a cypherlock, and only DFP personnel and selected cadets are provided access. All personnel will be reminded that this is a government computer system, subject to monitoring at all times, and all rules that apply to government computing apply to this lab. Maintenance of the rooms is the responsibility of DF Facilities.

2.1.1 Facility Description. The facility is located in Room 2A103 at 2354 Fairchild Dr., USAF Academy, CO 80840, though workstations used by associated personnel may be located in other parts of DFP. No special power or cooling requirements are needed. The departmental office area is secured with a cypherlock, and the room itself with a key. The combination to the cypherlock is maintained by the DFP Executive Officer. All DFP Personnel have access to the room, while senior physics majors and contractors will generally have access through workstations located elsewhere in the department.

2.1.2 Physical Security. Access to the facility is secured by a cypherlock and a key. In order to get the combination to the room, a request must be made to the DFP Executive Officer. Standard practice is that the combination is distributed among all DFP personnel. Combinations change on a yearly basis and when compromised.

2.1.3 Administrative Issues. Non-DFP personnel must request the cypherlock combination from the DFP Executive Officer or (in the case of the USAFA observatory) the Observatory Director before being allowed access to the lab.

2.1.4 Personnel. The WARF will be maintained primarily by its users. No special clearance is required. Also, janitorial workers will have periodic access in order to empty trash and vacuum. No special clearance is needed for them.

2.1.5 COMSEC. No special COMSEC procedures are required.

2.1.6 TEMPEST. The equipment and site are not required to meet TEMPEST requirements.

2.1.7 Maintenance Procedures. Routine maintenance will be conducted by DFP personnel through the normal CSRD process or by notifying the DF Facilities' job e-mail address. No extra personnel are required to provide lab maintenance.

2.1.8 Training. Training on the use of the facility will be conducted by the Principal Investigator or other qualified individuals with experience using the system.

2.2 Software development and maintenance environment. All applications in the lab are commercial products, shareware, or freeware. Software will be developed on an as needed basis as research and education are conducted.

2.3 Threat description. The WARF is subject to a range of generic threats applicable to most government information systems processing privacy act information. A potential threat exists to the confidentiality and integrity of the information processed, stored, and transmitted by the WARF. The potential threat to the LAN is from natural and manmade sources. Natural disasters and damage can result from fire, water, wind, and electrical sources. Manmade threats are from those who would target the USAFA LAN for espionage, criminal activity, unlawful use, denial of service, or malicious harm. External or internal agents of threat include espionage, terrorist, hackers, and vandals.

The most likely incident involves an authorized user who accidentally or inadvertently commits or omits some action that damages or compromises the system, one of its components, or information processed, stored, or transmitted by the WARF. The next most likely incident involves an authorized user who takes deliberate action to damage the WARF one of its components, or its data for personal gain or vengeful reasons. Also, there is a threat posed by users of the WARF who negligently or inadvertently fail to follow security requirements for the handling and labeling of system output or media, or the rules against the introduction of unauthorized software or data. Finally, there is the threat arising from the failure of authorized users to employ proper procedures for the entry or manipulation of system data arising due to failure of users to be properly trained in the use and operation of the WARF.

These insider threats can be manifested in the following ways:

- The unauthorized reading, copying or disclosure of sensitive information,
- The execution of denial of services attacks,
- The introduction into the system of viruses, worms or other malicious software,
- The destruction or corruption of data (intentional or unintentional),
- The exposure of sensitive data to compromise through the improper labeling or handling of printed output, or
- The improper labeling or handling of magnetic media resulting in the compromise of sensitive information.

3.0 SYSTEM ARCHITECTURAL DESCRIPTION

3.1 System Architecture Description. Hardware associated with the WARF includes servers, workstations, peripherals, and communications equipment required to exchange data within the WARF network. See Appendix E for drawing.

Linux Server (One only):
a. Dell Precision 420
b. 2 CPU, 933 MHz
c. 1 GB RAM
d. 133 GB disk
e. 19" color monitor
f. DLT tape drive
g. 4mm DAT tape drive

Other Server and Workstation Platform:
a. Dell system
b. Intel PIII, 450 MHz
c. 128 MB SDRAM
d. 10GB, 70GB hard drives
e. 19" SVGA Monitor

Peripherals:

a. 1 – HP Deskjet 930C Printer

3.2 System Interfaces and External Connections. The WARF be running a variety of COTS software and services that must be available to all machines on the lab network. Following are the applications:

Netscape 4.5 or higher
Star Office
KDE & Gnome Desktops
Apache Web Server

The following are the services that the WARF must provide; usage of these services will be in accordance with AFSSI 5027.

FTP
Telnet

3.3 Data Flow. All data passing from one group to another, or to and from a supporting system, must pass through the firewall for security mediation. The 10th CS has implemented an Access Control List at their router to monitor traffic to the WARF. The great majority of traffic will be in the form of downloads from web pages served by Archimedes.

3.4 Accreditation Boundary. The accreditation boundary can be seen by referencing Appendix E. Essentially, the WARF consists of the server Archimedes (together with printers, tape drives, etc. physically connected to that computer) and several additional workstations. All systems run RedHat Linux.

4.0 SYSTEM SECURITY REQUIREMENTS

4.1 **National and DOD Security Requirements.** The WARF shall comply with requirements specified in Air Force Instruction, Air Force System Security Instruction, and DoD 5200.28-STD. Requirements articulated in DoD 5200.28-STD are validated by Federal Information Processing Standards (FIPS) publications, Office of Management and Budget circulars and bulletins, Executive Orders, US legislative documents.

4.2 **Governing Security Requirements.** The Department of Defense requirements are found in DoD Directive 5200.28 Telecommunication and Automated Information Systems Security. This is the primary DOD implementation of the national security policy for AIS security. Other related DOD Directives and Instructions are listed below:

5 CFR Part 930
28 CFR Part 17 - National Security Information Program
Computer Security Act of 1987 (P.L. 100-235), 8 January 1988
OMB Circular A-123, Management Accountability and Control, June 21, 1995
OMB Circular A-130, Management of Federal Information Resources, Appendix III - Security of Federal Automated Information Resources, February 16, 1996
OMB Bulletin 90-08, Individual Security Plan Guidance
NACSIM 7000 TEMPEST
DoD 5200.28-STD Trusted Computer System Evaluation Criteria (TCSEC)
Director of Central Intelligence Directive (DCID) 1/16
National Security Agency (NSA) Manual 90-2, "COMSEC Material Control Manual"
The Trusted Network Interpretation (TNI) of the TCSEC, National Computer Security Center Technical Guide 005 (NCSC-TG-005)
FIPS Publication 46-2, Data Encryption Standard
FIPS Publication 65, Guideline for Automatic Data Processing Risk Analysis
FIPS Publication 81, DES Modes of Operation
FIPS Publication 83, Guidelines on User Authentication Techniques
FIPS Publication 87, Guideline for ADP Contingency Planning
FIPS Publication 102, Guideline for Computer Security Certification and Accreditation
FIPS Publication 112, Standard on Password Usage
FIPS Publication 191, Guideline for the Analysis of Local Area Network Security
National Bureau of Standards (NBS) Special Publication 500-137, Security for Dial-Up Lines
NBS Special Publication 500-153, Guidelines to Auditing for Control and Security: A Developmental Life Cycle Approach
USAFA Network Security Policy
Air Force Network Security Policies

4.3 **Data Security Requirements.** The type of data processed by the WARF does not require any special handling or additional protection.

4.4 **Security CONOPS.** The purpose of the facility is education and research. Basic system security will be provided by the 10th CS router. Users and administrators will maintain password-protected access to the system in accordance with AFSSI 5027, and relevant Linux security patches will be installed as they become available. Services not generally required (such as anonymous ftp) will be disabled.

The WARF will be connected to the internet, and most users outside the security perimeter will access data files via http/ftp. For those projects or procedures that require internet connectivity, host-security software will be installed and running on the machine that is connected to the internet, and researchers will be responsible for ensuring the security of the entire network or at least for the portion of the network that they are utilizing.

4.5 Network Connection Rules. The connection of the WARF to any other network not mentioned in this SSAA must have prior approval from the 10th CS.

4.6 Configuration Management. DFP must evaluate the impact to security for all changes (hardware, software, and firmware) to the system.

4.7 Reaccreditation Requirements. This SSAA and all security documentation shall be reviewed and revised as appropriate under the following circumstances:

- Significant changes in the hardware, software, or data communications configuration.
- Changes in the security mode of operation.
- Relocation or structural modifications of the computer facility or remote terminal area.
- A breach of security, violation of system integrity, or unusual situation that appears to invalidate the certification.
- Three years have elapsed since the date of certification.

5.0 ORGANIZATIONS AND RESOURCES

5.1 Organizations. Key personnel involved in the C&A process for the WARF are:

Department of Physics (DFP):
WARF Director: Dr. Derek Buzasi, 333-4570

5.2 Resources. No outside or additional resources will be required to complete the C&A process for the WARF.

5.3 Training. No additional training is required in order to support and maintain the WARF.

5.4 Other supporting organizations. None

6.0 DITSCAP PLAN

6.1 Tailoring factors.

6.1.1 Programmatic considerations. Programmatic considerations are a tailoring factor not applicable to the WARF.

6.1.2 Security environment. Physical security is addressed by being located behind a cypher locked door. Users and administrators will maintain password-protected access to the system in accordance with AFSSI 5027, and relevant Linux security patches will be installed as they become available. Services not generally required (such as anonymous ftp) will be disabled.

6.1.3 IT system characteristics. The WARF employs a Dell commercial hardware platform running Red Hat Linux OS. The software applications used are universally available commercial programs. Communications connectivity involves well-known and understood components such as a CISCO router, and Ethernet hub. No unusual, experimental, or new model components complicate the information system environment.

6.1.4 Reuse of previously approved solutions. Reuse of previously approved solutions is a tailoring factor not applicable to the WARF.

6.2 Tasks and milestones. A security test will be performed within 3 months after interim accreditation is granted.

6.3 Schedule summary. 10CS/SCBI (Information Assurance Office) will provide draft Letter of Certification for signature. Once signed, 10CS/SCBI will staff the Letter of Certification, the SSAA, and the Letter of Accreditation to the Designated Approval Authority (USAFA/DAA) to request Interim Accreditation. Upon approval of Interim Accreditation, the system will be authorized to operate for period of three months. During this three month period, a security test of the system must be performed and a risk analysis completed. The risk analysis will be forwarded with updated SSAA for consideration of full accreditation.

6.4 Level of effort. There are sufficient resources available to complete the Certification and Accreditation process, and provide management of the WARF.

6.5 Roles and responsibilities. DFP will primarily be responsible for the development, execution, and maintenance of the SSAA. The key personnel are:

Department of Physics (DFP):
WARF Director: Dr. Derek Buzasi, 333-4570

The 10th CS will primarily be responsible for the evaluation of the SSAA.

APPENDIX A. Acronym list

ACL:	Access Control List
CDE:	Cyber Defense Exercise
IA/IW:	Information Assurance/Information Warfare
IA-PERL:	Information Assurance – PKI Education & Research Lab
LIWA:	Land Information Warfare Agency
NASA:	National Aeronautics and Space Administration
NSA:	National Security Agency
NSSDC:	National Space Science Data Center
PKI:	Public Key Infrastructure
PMO:	Program Management Office
SSAA:	System Security Authorization Agreement
USAFA:	United States Air Force Academy
VPN:	Virtual Private Network
WIRE:	Wide-Field Infrared Explorer satellite
WWW:	World-Wide Web

APPENDIX B. Definitions

The terms used in this document were selected from the NSTISSI 4009 (reference(i)) definitions when possible. Where new terms are used, the revised or new definitions will be submitted as changes to reference (i).

Accountability. Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation.

Accreditation. Formal declaration by a DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards.

Architecture. The configuration of 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 or information; includes computers, ancillary equipment, and services, including support services and related resources.

Acquisition Organization. The Government organization responsible for developing a system.

Active System. A system connected directly to one or more other systems. Active systems are physically connected and have a logical relationship to other systems.

Assurance. Measure of confidence that the security features and architecture of an IT system accurately mediates and enforces the security policy.

Authenticity. The property that allows the ability to validate the claimed identity of a system entity.

Availability. The property of a resource being accessible and usable upon demand by an authorized user.

Audit. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Benign System. A system that is not related to any other system. Benign systems are closed communities without physical connection or logical relationship to any other system. Benign systems are operated exclusive of one another and do not share users, information, or end processing with other systems.

Certification. Comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards made in support of the accreditation process to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certification Authority (CA). The official responsible for performing the comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards made in support of the accreditation process to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Compartmented Mode. INFOSEC mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all the following: a. Valid security clearance for the most restricted information processed in the system; b. Formal access approval and signed non-disclosure agreements for that information to which a user is to have access; and c. Valid need-to-know for information to which a user is to have access.

Computing Environment. The total environment in which an automated information system, network, or a component operates. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other information systems.

COMSEC. Communications Security. Measures and controls established to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Note: Communications security includes cryptographic security, transmission security, emission security, and physical security of COMSEC material.

Confidentiality. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration Control. Process of controlling modifications to an IT system's hardware, firmware, software, and documentation to ensure that the system is protected against improper modifications prior to, during, and after system implementation.

Configuration Management. Management of security features and assurances through control of changes made to hardware, firmware, software, documentation, test, test fixtures, and test documentation of an automated information system throughout the development and operational life of a system.

Configuration Manager. The individual or organization responsible for configuration control or configuration management.

Data Integrity. The attribute of data relating to the preservation of (1) its meaning and completeness; (2) the consistency of its representation(s); and (3) its correspondence to what it represents.

Dedicated Mode. IT security mode of operation in which each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has the following:

- Valid security clearance for all information within the system.

- Formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments and/or special access programs).

- Valid need-to-know for all information contained within the IT.

Defense Information Infrastructure (DII). The DII encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the DoD's local and worldwide information needs. The DII connects DoD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and provides information processing and value-added services to subscribers over the DISN. Unique user data, information, and user applications software are not considered part of the DII.

Designated Approving Authority (DAA - Accreditor). Official with the authority to formally assume the responsibility for operating an IT system or network at an acceptable level of risk.

Developer. The organization that develops the information system.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information system security activities.

Emissions Security (EMSEC). Protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from crypto-equipment or an information system.

Environment. The aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system.

Evolutionary Program Strategies. Generally characterized by design, development, and deployment of a preliminary capability that includes provisions for the evolutionary addition of future functionality and changes, as requirements are further defined.

Governing Security Requisites. Those security requirements that must be addressed in all systems. These requirements are set by policy, directive, or common practice set, e.g., by Executive Order, OMB, Office of the Secretary of Defense, a military service or DoD agency. They are typically high-level. While their implementations will vary from case to case, these requisites are fundamental and must be addressed.

Grand Design Program Strategies. Characterized by acquisition, development, and deployment of the total functional capability in a single increment.

Incremental Program Strategies. Characterized by acquisition, development, and deployment of functionality through a number of clearly defined system "increments" that stand on their own.
Information Category. The term used to bound information and tie it to an information security policy.

Infrastructure-Centric. A security management approach that considers information systems and their computing environment as a single entity.

Information Integrity. The preservation of unaltered states as information is transferred through the system and between components.

Information Operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Security Policy. The aggregate of directives, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information. For example, the information security policy for financial data processed on DoD systems can be contained in public law, executive orders, DoD directives and local regulations. The information security policy lists all the security requirements applicable to specific information.

Information System. Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data; includes software, firmware, and hardware.

Information System Security Officer (ISSO). The person responsible to the DAA who ensures that an IT system is approved, operated, and maintained in accordance with the SSAA.

Information Technology (IT). The hardware, firmware, and software used as part of the information system to perform DoD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Information Technology Security (ITSEC). Protection and maintenance of confidentiality, integrity, availability, and accountability.

Integrator. The organization that integrates the information system components.

Integrity. The property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing service to function according to specified expectations. It is composed of data integrity and system integrity.

Interim Approval To Operate. The system does not meet the requirements as stated in the SSAA, but mission criticality mandates the system become operational. The IATO is a temporary approval which may be issued for no more than a one-year period.

Legacy Information System. An operational information system that existed prior to the implementation of this process.

Maintainer. The organization that maintains the information system.

Maintenance Organization. The Government organization responsible for the maintenance of an IT system. (Although the actual organization performing maintenance on a system may be a contractor, the maintenance organization is the Government organization responsible for the maintenance.)

Mission Justification. The description of the operational capabilities required to perform an assigned mission. This includes a description of a system's capabilities, functions, interfaces, information processed, operational organizations supported, and the intended operational environment.

Multilevel Secure Mode. IT security mode of operation in which the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts:

- Some users do not have a valid security clearance for all information processed in the IT.

- All users have the proper security clearance and appropriate formal access approval for that information to which they have access.

- All users have access only to information for which they have a valid need-to-know.

Mission. The assigned duties to be performed by a resource.

Non-Developmental Item (NDI). Any item that is available in the commercial marketplace; any previously developed item that is in use by a department or agency of the United States, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; any item described above that requires only minor modifications in order to meet the requirements of the procuring agency; or any item that is currently being produced that does not meet the requirements of definitions above, solely because the item is not yet in use or is not yet available in the commercial marketplace.

Operational Security (OPSEC). Process denying information to adversaries about capabilities and/or intentions by identifying, controlling, and protecting unclassified generic activities.

Other Program Strategies. Strategies intended to encompass variations and/or combinations of the Grand Design, Incremental, Evolutionary, or other program strategies.

Passive System. A system related indirectly to other systems. Passive systems may or may not have a physical connection to other systems, and their logical connection is controlled tightly.

Program Manager. The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT system.

Residual Risk. Poation of risk remaining after security measures have been applied.

Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.

Risk Assessment. Process of analyzing threats to and vulnerabilities of an IT system, and the potential impact that the loss of information or capabilities of a system would have on a national security and using the analysis as a basis for identifying appropriate and cost-effective measures.

Risk Management. Process concerned with the identification, measurement, control, and minimization of security risks in IT systems.

Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

Security Inspection. Examination of an IT system to determine compliance with security policy, procedures, and practices.

Security Process. The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life-cycle.

Security Requirements. Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

Security Requirements Baseline. Description of the minimum requirements necessary for an IT to maintain an acceptable level of security.

Security Specification. Detailed description of the safeguards required to protect an IT system.

Security Test and Evaluation (ST&E). Examination and analysis of the safeguards required to protect an IT system, as they have been applied in an operational environment, to determine the security posture of that system.

Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S. C. Section 552a, but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

System. The set of interrelated components consisting of mission, environment, and architecture as a whole.

System Entity. A system subject (user or process) or object.

System Integrity. The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System High Mode. IT security mode of operation in which each user with direct or indirect access to the IT, its peripherals, remote terminals, or remote hosts, has all of the following:

- Valid security clearance for all information within an IT.

- Formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, and special access programs).

- Valid need-to-know for some of the information contained in the IT.

- System Security Authorization Agreement (SSAA). The SSAA is a formal agreement among the DAA(s), the CA, the IT system user representative, and the program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify ITSEC requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

TEMPEST. Short name referring to investigation, study, and control of compromising emanations from IT equipment.

Threat. Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to, information or an information system.

Threat Assessment. Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Trusted Computing Base (TCB). Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

User. The individual or organization that operates or uses the resources of an information system.

User Representative. The individual or organization that represents the user or user community in the definition of information system requirements.

Utility. An element of the DII providing information services to DoD users. These services include Defense Information Systems Agency Megacenters, information processing, and wide area network communications services.

Validation. Determination of the correct implementation in the completed IT system with the security requirements and approach agreed upon by the users, acquisition authority, and DAA.

Verification. The process of determining the compliance of the evolving IT system specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and DAA.

Vulnerability. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited.

Vulnerability Assessment. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

APPENDIX C. References

Office of Assistant Secretary of Defense Memorandum, The Defense Information Systems Security Program (DISSP), August 19, 1992.

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

Public Law 100-235, "Computer Security Act of 1987," January 8, 1988

Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1996

Director of Central Intelligence 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks," March 14, 1988

DoD Directive 5220.22, "Industrial Security Program," November 1, 1986.

DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP), DoD Instruction 5200.40, 30 December 1997.

DoD Regulation 5000.2-R, Mandatory Procedures for Major Defense Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs, November 4, 1996.

National Information Systems Security (INFOSEC) Glossary, NSTISSI 4009, August 1997

An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12, October 1995.

The Certification and Accreditation Process Handbook for Certifiers, NCSC-TG-031, Draft, July 1996[1]

Management Accountability and Control, OMB A-123, June 21, 1995.

Accreditors Guideline, NCSC-TG-032, Draft July 1997[2]

Systems Engineering Management Guide, Defense Systems Management College, January 1990.

Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, NIST Special Publication 800-4, March 1992.

Trusted Database Management System Interpretation, NCSC-TG-021, Version 1, April 1991.

Assessing Controlled Access Protection, NCSC-TG-028, Version 1, May 25, 1992.

A Guide to Understanding Design Documentation in Trusted Systems, NCSC-TG-007, Version 1, October 2, 1988.

Trusted network Interpretation Environments Guideline, NCSC-TG-011, Version 1, August 1, 1990.

A Guide to Understanding Trusted Recovery in Trusted Systems, NCSC-TG-022, Version 1, December 30, 1991.

Guideline for Life-cycle Validation, Verification, and Testing of Computer Software, FIPS Publication 101, June 6, 1983.

Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards, NIST Special Publication 500-165, September 1989.

Automated Tools for Testing Computer System Vulnerability, NIST Special Publication 800-6, December 1992.

A Guide to Understanding Audit in Trusted Systems, NCSC-TG-001, Version 2, June 1, 1988.

A Guide to Understanding Discretionary Access Control in Trusted Systems, NCSC-TG-003, Version 1, September 30, 1987.

A Guide to Understanding Identification and Authentication in Trusted Systems, NCSC-TG-017, Version 1, National Computer Security Center, September 1991.

A Guide to Understanding Object Reuse in Trusted Systems, NCSC-TG-018, Version 1, July 1, 1991.

Configuration Management Military Standard, MIL-STD-973, April 17, 1992.

A Guide to Understanding Configuration Management in Trusted Systems, NCSC-TG-006, Version 1, March 28, 1988.

[1] Available from the DISA Information Systems Security Program Management Office, 701 Courthouse Road, Arlington, VA 22204-2199.

[2] Available from the DISA Information Systems Security Program Management Office, 701 Courthouse Road, Arlington, VA 22204-2199.

A Guide to Understanding Trusted Distribution in Trusted Systems, NCSC-TG-008, Version 1, December 18, 1988.

Rating Maintenance Phase Program Documentation (NCSC-TG-013).

A Guide to Understanding Trusted Facility Management, NCSC-TG-015, Version 1, October 18, 1989.

Guidelines for Automatic Data Processing Physical and Risk Management, FIPS Publication 31, June 1974.

Guideline for Automatic Data Processing Risk Analysis, FIPS Publication 65, August 1, 1993.

Laboratory TEMPEST Test Standard, NSTISSAM TEMPEST/1-92.

Compromising Emanations Field Test Requirements, Electromagnetics, NSTISSAM TEMPEST/1-93, August 30, 1993.

Procedures for TEMPEST Zoning, NSTISSAM TEMPEST/2-92, December 30, 1992.

Guidelines for Facility Design and RED/BLACK Installation, NACSIM 5203, June 1, 1982.

Communications Security (COMSEC), DOD Directive C-5200.5, October 6, 1981.

Defense Special Security Communications: Security Criteria and Telecommunications Guidance, DOD-C5030.58-M, July 1978.

Communications Security (COMSEC) Monitoring, NTISSD 600, April 10, 1990.

INFOSEC Software Engineering Standards and Practices Manual, NSA DS-80, January 9, 1991.

Computer Security Guidelines for Implementing the Privacy Act of 1974, FIPS Publication 41, May 30, 1975.

Guidelines on Evaluation of Techniques for Automated Personal Identification, FIPS Publication 48, April 1, 1977.

Guidelines for Security of Computer Applications, FIPS Publication 73, June 30, 1980

Guideline on User Authentication Techniques for Computer Network Access Control, FIPS Publication 83, September 29, 1980.

Guidelines for ADP Contingency Planning, FIPS Publication 87, March 27, 1981.

Guideline for Computer Security Certification and Accreditation, FIPS Publication 102, September 27, 1988.

Password Usage, FIPS Publication 112, May 30, 1985.

Computer Data Authentication, FIPS Publication 113, May 30, 1985.

Defense Acquisition, DoD Directive 5000.1, March 15, 1996.

Memorandum on Information Management Definitions issued by the Assistant Secretary, 26 February 1994.

Subsection 552a of title 5, United States Code.

Department of Defense Technical Architecture Framework for Information Management (TAFIM), Volume 6, DoD Goal Security Architecture (DGSA), 30 April 1996[3]

AFI 33-112, Automated Data Processing Equipment (ADPE) Management, 1 Dec 97

AFI 33-114, Software Management, 30 Jun 94

AFI 33-115, Network Management, 1 Apr 96

AFI 33-129, Transmission of Information via the Internet, 1 Jan 97

AFI 33-202, The Computer Security Program, 1 Feb 1999

AFI 33-204, Security Awareness Education and Training, 1 Oct 97

AFMAN 10-401, Operation Plan and Concept Plan Development and Implementation, 1May 98

AFMAN 33-223, Identification and Authentication, 1 Jun 98

AFPD 33-2, Information Protection, 1 Dec 96

AFSSI 5020, Remanence Security, 20 Aug 96

AFSSI 5021, Vulnerability and Incident Reporting, 15 Aug 96

AFSSI 5024, Volume I The Certification and Accreditation Process, 1 Sep 97
Volume II The Certifying Official's Handbook, 1 Sep 97
Volume III The Designated Approving Authority Guide, 1 Mar 99
Volume IV Type Accreditation, 1 Mar 99

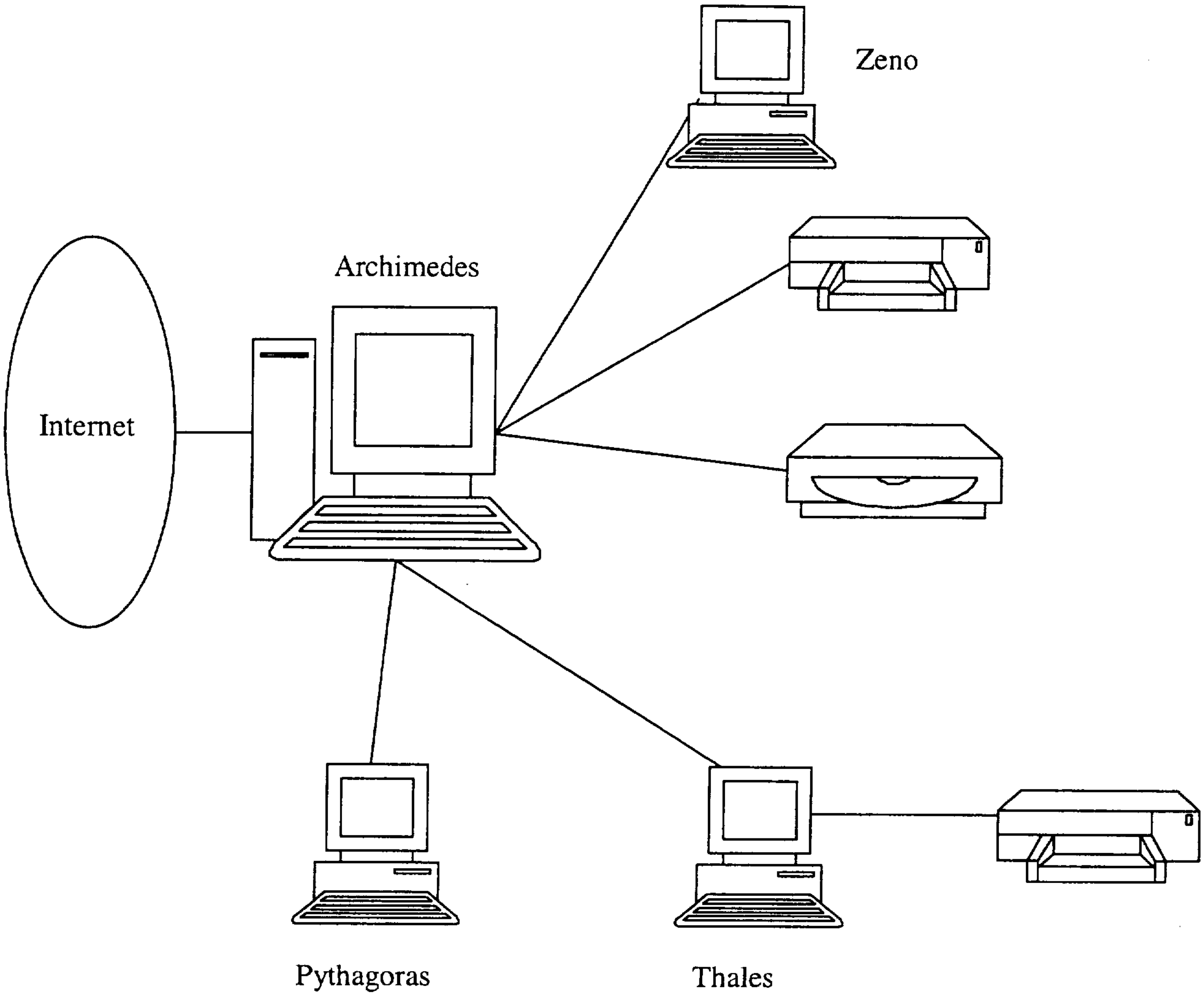
AFSSI 5027, Network Security Policy, 27 Feb 98

[3] Available from the DISA Information Systems Security Program Management Office, 701 Courthouse Road, Arlington, VA 22204-2199.

APPENDIX D. Trusted Facility Manual

[redacted]

APPENDIX E. Topology



APPENDIX G. Contingency Plan

Major system backups will be performed monthly, using the DLT tape drive attached to Archimedes. In addition, the data archive will be separately maintained on DLT tape and eventually mirrored at the NSSDC. In the event of system failure, the tape backups will be used to reconstitute the system. Should Archimedes undergo a catastrophic hardware failure, any of the other workstations in the WARF will be reconfigurable to serve its function.