Global Information Assurance Certification Paper

Testing, Certifying, and Approving Information Systems-One Perspective

Joseph R Parra
December 17, 2000

This paper does not intend to give the allusion of an all-inclusive process to certifying, testing, and obtaining an approval for operation of an Information Technology (IT) system. It does however present a viewpoint on how to proceed with these actions and to at least formulate the plans, which are required to perform this necessary process. Information will be provided that will or should give the basic steps that should be followed when attempting to remove or identify much of the significant risk areas and provide; not only to the user, but to the approving authority a well tested IT system. Certifying the tested system follows closely to the testing aspect in that most action taken are at one point or another agreed upon by a testing team and, depending on how test plans are written, certified or attested to correctness or behavior of operations of the IT system.

All systems should undergo a Testing and Certification (T&C) before they can be approved for operation in accordance with corporate or other regulatory guidance. Some examples of Federal guidance are listed as references. Enclosure A is an example of a generic outline for T&C plans. Enclosure B is a sample checklist for IT system certification requirements or checks that are considered to be an absolute minimum. Best-commercial-practice tools commonly utilized to achieve quantified, operational determination of IT architecture and system operational compliance are listed in Enclosure C. Enclosure D is a generic outline for IT systems T&C reports.

Many agencies and business ordinarily use T&C to quantify and document the extent to which there IT system is or provides protection of information. This paper provides only a process that can form the core of IT system T&C. Since many resources can be consumed during and preceding these actions it is best to plan in advance and to make every effort to make the best use of the information obtained. Pre-planning will eliminate many hours' of effort later as T&C proceeds.

The T&C process begins with the requirement that were to be met for the system development. Since, in most cases these requirements are either lacking or non-existent, a thorough description of the system, its boundaries, and its operating environment (based on whatever documentation is available—-essentially a discovery process) is an absolute necessity. A determination of the system's mission reliance factor and the sensitivity of the information processed on the system have to be stated. Next, a determination is made as to whether appropriate security policies have been followed by applying appropriate threat descriptions and hands-on testing of the system. This is followed by IT risk and vulnerability assessments. It is important to note that the metrics provided from rigorous system tests present management with the operationally-quantified, up-to-the-moment information as to the health or compliance of an IT system.

Applying a process to the IT environment is the primary concern. An assumption is that the IT system has not previously been approved or the process used previously for approval was flawed to dated. This deficiency could place the network or the total operational environment at risk of being compromised. Without T&C (and the approval process), there is no security "baseline" nor is there documentation of the security processes.

Roles and Responsibilities have to be identified in the beginning. Not only is it imperative that these duties be identified but that qualified people be selected to be team members. Again, remember that this can be resource intensive so it is best to plan and allow for possible delays.

Security Support Staff

The Security Support Staff is responsible for ensuring that the IT system operates in a secure hardware and software electronic environment in accordance with stipulated regulatory guidance.

In close consultation and cooperation with the Information Technology Staff, the Security Support Staff are responsible for ensuring that appropriate T&C are carried out and followed (through planning, coordinating, and/or conducting) so as to operationally quantify the security posture of the IT system/environment. Tests include (but may not be limited to):

- operational determination/confirmation of the architecture;
- operational assessment of the IT system vulnerabilities; and
- operational assessment of risks to the IT system/environment

T&C is a necessary first step in the line of defense for an IT system/environment. It identifies, clarifies and/or establishes security policies, practices, and procedures; it is also an ongoing process performed periodically over the life cycle of the IT system/environment.

The Security Support Staff is responsible for post-test completion of the certification process. The process consists of documenting all test results (and supporting information) as required by the specific process followed for the IT system (generally Authorization Agreement or an Approval Document/Letter).

The Security Support Staff is responsible for coordinating the preparation of the Authorization Agreement or the Approval Document/Letter or documentation package for the final approval by the person or persons who will acknowledge responsibility and or ownership of the system, its operation, and its T&C security posture.

Information Technology Division

The Information Technology Division is responsible for providing a current architecture of the IT system with supporting documentation to the Security Support Staff. Ownership and operation of the IT system generally resides within the office of the Chief Information Officer and the Information Technology Division.

The Information Technology Division is responsible for maintaining configuration of the IT system once that system has been approved. The IT Division is also responsible for configuration management of the IT system and for providing documentation of proposed IT system configuration changes (prior to implementation of such changes) to the Security Support Staff in a timely manner. The Security Support Staff will use this information to advise the Information Technology Division (usually within less than five working days) on maintaining a secure electronic environment as well as to determine if and when the IT system should be re-tested and certified.

In conclusion, any effort that consumes resources is always questionable. The return on the investment for the T&C are and can be measured in many ways. Many reports circulate the news forums daily on attacks against network and other IT assets of the corporate world. Testing and Certification can fall within a gray "not needed" area of not needed. Evidence has shown that with a good process in place to Test and Certify systems many of the attacks that are experienced today can and would be avoided. To this end plans and processes that are developed and executed and then follow by continual maintenance and observation of system performance and protective elements will bring the benefits that were in the beginning somewhat gray area. The significant contribution and conclusion of a successful T&C is the measurement of the risk the IT system was exposed to prior to testing and the efforts taken to either reduce this risk or many cases mitigate the risk to an acceptable level.

References

[1] Department of Defense Directive 5200.28, Security Requirements for Automated Information Systems, March 21, 1988

[2] Department of Defense Instruction 5200.40, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997

[3] Army Regulation 380-53, Information Systems Security Monitoring, Annex A, April 29 1998

[4] Office of Management and Budget Circular No. A-130

Enclosures

[A] Test & Certification Plan

[B] Test & Certification Check List (source unknown)

[C] Test & Evaluation Tools for Operational Certification of System Architecture

[D] Test & Certification Report

ENCLOSURE A

TEST & CERTIFICATION (T&C) PLAN

1. Responsible Organization

2. Level of Effort

   2.1 Minimal/Moderate or Extensive
   2.2 Justification

3. T&C Team Composition/Roles & Responsibilities

   3.1 Identification of T&C Team Members
   3.2 Roles and Responsibilities

4. Assumptions, Constraints, and Dependencies

   4.1 Assumptions
   4.2 Constraints
   4.3 Dependencies

5. Test Procedures (for extensive T&C, for minimal and moderate T&C, use T&C Checklist)

   5.1 Requirement or Policy Statement Being Tested
   5.2 Objective
   5.3 Scenario
   5.4 Expected Results

6. T&C Schedule

The schedule will consist of a timeline for the conducting of the T&C.

ENCLOSURE B

TEST & CERTIFICATION CHECK LIST FOR MINIMAL/MODERATE LEVEL OF EFFORT

#	Test	Test Method	Yes	No	N/A
Passwords					
1.	Do all users have unique passwords?	I			
2.	Are passwords masked to prevent casual viewing when logging in?	D			
3.	Are password files encrypted?	I			
4.	Can alphanumeric characters be used to generate passwords?	T			
5.	Are passwords required to be at least 8 characters long?	T			
6.	Are passwords encrypted between server and workstation during the login process?	I			
7.	Besides the administrator, is the user the only person who can make a permanent change in their password?	T			
8.	Are Guest account disabled?	I			
9.	To generate a password, the system can use the following character sets: (please circle all that apply): Uppercase letters Lowercase letters Numbers More than 8 characters At least 8 characters	T			
10.	Are passwords generated at random?	A			
11.	Are procedures in place to ensure that dictionary-type words are not used as passwords?	D			
12.	Are passwords changed at least every 90 days	I			
13.	Are password histories utilized to prevent users from immediately reusing the old password?	I			
14.	Are passwords given an expiration or "must change" date?	I			
15.	Does each user's terminal have a screen lock function that can be invoked by the user, or after 10 minutes of terminal inactivity?	I			
16.	Are all users required to initially login using their individual userid and password before switching to group accounts? a) Is this policy enforced by the system?	T			
17.	Are passwords or other similar access controls for individual users changed or deleted when: a) User access is withdrawn for any reason? b) There has been a compromise or a suspected compromise of the password or access control?	I			

18.	Are access control mechanisms properly protected? a) For unclassified (non-sensitive) systems, are the passwords or other access controls (authenticators) protected at the minimum of "For Official Use Only"? b) For sensitive and classified systems, are the passwords or other access control mechanisms (authenticators) protected at the same sensitivity level as the data accessed by the password or control mechanism?	T			
Virus Management					
1.	Anti-viral software is used on the workstations	I			
2.	Anti-viral software is used on the servers	I			
3.	Floppies are scanned for viruses before being introduced to the system	I			
4.	There is a posted procedure in place for reporting viruses	I			
5.	There is an active virus awareness program established and enforced	A			
6.	Backups of software for critical applications are compared to working copies to detect unauthorized changes	D			
Education & Training					
7.	There is an education and awareness program in place	I			
8.	Are CERT advisories and alerts circulated?	I			
9.	Do all personnel have a security brief at least quarterly?	I			
10.	Does the ISSO have the proper training?	D			
11.	Does the ISSO provide initial security training to newly assigned personnel?	D			
12.	Does the ISSO provide periodic security training to all system users?	I			
13.	Is security awareness material (e.g., security briefings, films, posters) evident and appropriate for the operating environment?	I			
14.	Are procedures in place to provide temporary assigned personnel training?	I			
Electrical Hazards					
15.	Are uninterrupted power supplies (UPS) utilized on all workstations?	I			
16.	Are uninterrupted power supplies (UPS) utilized on all servers?				
17.	If auxiliary generators are required due to the criticality of the mission, have they been provided?	I			
18.	Are electromechanical door locks and fire alarms backed up with battery power in case of a power failure?	I			
19.	If available, is back-up power-off tested at regular intervals? a) If tested, are the tests documented?	I			
20.	Are emergency power switches protected from accidental activation?	I			
21.	Have all known security deficiencies involving electrical power been corrected?	I			
Labeling					
22.	Is all output properly marked with the appropriate sensitivity (classification & category) markings (e.g., Privacy Act, FOUO, Source Selection Sensitive, Confidential, Secret)?	I			

23.	Are effective policies in place to make sure the user is responsible for: a) Verifying that no extraneous data has been included in their output products? b) Verifying that the classification level indicated on the product is consistent with that assigned to the data by the user? c) Reporting all security discrepancies to the ISSO, TASO, or other designated representative?	I			
24.	Are effective policies established to ensure that any removable magnetic media are marked on the visible portion of the media with any classification/category or special handling instructions? a) Are classified equipment and removable storage media (e.g., tapes, and disks) labeled in accordance with established policy? b) Do the labels show: 1) The name of the owner of the data? 2) The creation date? 3) Any classification or special handling or access instructions? 4) A description of the contents? 5) Any control/inventory numbers? 6) A color code or coded label?	I			
25.	Are there procedures in place to account for all: a) Fixed mass storage media (disk, core, system files)? b) Removable storage media (disk or tape)?	I			
26.	Are periodic site inventories of all removable media conducted?	I			
27.	Are all media used for the restoration of the operating system protected against unauthorized modifications? a) Are backup copies maintained off site? b) If an off-site facility is used, does this facility meet all of the security requirements for the media (physical, administrative, procedural, etc.)? c) Are accountability procedures in place to ensure that only authorized users gain access? d) Are system audit media likewise protected?	T			
28.	Are security procedures in place: a) Mailing removable media? b) Locally transporting removable media? c) Verifying that the intended destination received the media shipped? d) Maintaining the physical security requirements associated with the media?	D			
29.	Are all magnetic media that contained classified or sensitive but unclassified information degaussed prior to being released for reused, destroyed, or salvaged?	I			
30.	Are all removable media controlled at the highest level of sensitivity of the information processed or stored?	T			
31.	If the systems media contain classified or sensitive/critical tables, files, or routines, are they protected at the highest sensitivity of the data?	I			
32.	Is there a method in place to control access to the system storage media?	T			
33.	Is the ISSO notified of any unauthorized attempts or requests to access the system storage media?	T			
34.	Have procedures been established for the proper disposal/destruction of system products (e.g., listings, disks, tapes, and microfilm)?	D			

Personnel Security					
35.	Have procedures been established for requesting an account?	D			
36.	Are individuals given only the minimum capabilities required to perform their assigned duties?	I			
37.	Do all personnel gaining access to the system have a need to know for all information to which they are granted access?	A			
38.	Is access to the system canceled when individuals leave or no longer need access?	I			
39.	Are personnel clearances appropriate for the operating environment?	I			
40.	Are background checks reaccomplished periodically?	I			
41.	Are supervisors notified immediately when an employee is placed on a control roster, has an unfavorable information file opened, is under investigation by a law enforcement agency, or becomes disgruntled?	I			
42.	Do personnel policies allow for removal or temporary reassignment of employees who are experiencing personal difficulties or who are undergoing medical treatment?	I			
43.	Has each employee with access to sensitive programs and/or data signed the appropriate confidentiality agreements?	I			
44.	As personnel leave the organization, are those employees who had access to sensitive information informed of their obligation to return any copies of such information that might be in their possession and to protect all such information even after they leave?	I			
45.	Does the facility have a current roster of personnel assigned permanently to the facility or to organizations utilizing the facility?	I			
46.	Are there procedures for notifying security guards or personnel who control access to the facility when personnel are debriefed or have left the organization?	I			
47.	Are escort procedures established for all visitors (e.g., maintenance personnel)?	I			
48.	Does the facility maintain a cleared visitor roster or file of current visitation request forms?	I			
49.	Has the cleared visitor roster/visitation requests been certified or verified by the appropriate security official?	I			
50.	Have the names of visitors whose visit requests/clearances have expired been removed from roster?	I			
51.	Are access control procedures for maintenance and custodial personnel appropriate for the operating environment?	I			
52.	When hardware maintenance personnel are not cleared, are they escorted and watched to ensure that they do not remove sensitive or classified equipment, insert unauthorized devices, or otherwise violate security?	I			
53.	Are all personnel cleared who have unescorted access to workstations, displays, and printers, for example?	I			
54.	Do personnel ensure that no sensitive and/or classified data are removed from the facilities?	I			
55.	An access list is displayed	I			
56.	Unauthorized users are challenged and denied access to the systems and peripherals	I			
57.	Are all terminal areas physically secured at the end of the day?	T			

58.	Are information system hardware and software protected against theft? a) Are administrative and physical controls in place to ensure that portable terminals are not stolen or misused?	T			
59.	Are positive personnel identification measures (e.g., badge system, fingerprints) in place?	I			
60.	Are visitors to the facility easy to identify (i.e., badge system or personal recognition) or challenged for identification and purpose of visit?	I			
61.	Have security personnel and operators been briefed on how to respond to such events as bomb threats, arson or sabotage threats, or reports of fraud, vandalism, or abuse? a) Are checklists/operating instructions available to identify actions necessary in the case of such events? b) Are periodic exercises conducted? c) Do personnel know to whom to report such events?	D			
62.	Is access to the computer facility limited to personnel who have a justifiable need for access?	I			
63.	Are keys, electromechanical locks, or other security devices used to control facility access? a) If keys are used, are they formally signed out? b) If keys are used, are they collected from employees upon termination or relocation?	I			
64.	Are the keys and locks or combinations changed periodically and after the termination/reassignment of employees?	I			
65.	Are procedures in place to maintain physical security commensurate with the highest classification/sensitivity of information processed or stored by the system?	I			
Security Incident Reports					
66.	Are all security incidents investigated to determine their cause? Are corrective actions taken to the extent possible?	I			
67.	Are formal investigations conducted whenever a compromise, or suspected compromise, of classified information results from a security incident?	I			
68.	Have files been established for incident reports? a) Are there procedures established to report incidents? b) Are there procedures to file incident report information? c) Does the ISSO review the incident report files to ensure timely follow-up?	I			
Downgrading, Erasure & Sanitization Controls					
1.	Is each memory location used for the storage of classified or sensitive data overwritten when it is no longer required, before reuse by the system, or before the contents of the location may be accessed by any subsequent process? (This refers to object reuse requirement.)	I			
2.	Does the ISSO approve and verify the sanitization of all sensitive equipment?	I			
3.	Are the available magnetic tape erasure (i.e., degaussers) models approved by NSA?	I			

4.	Do procedures exist to ensure that all memory is cleared between periods processing that involve classified data? (Note: clear memory if new processing level is the same or higher than previous level; otherwise memory must be purged.)	D			
5.	Is all removal magnetic media used to store sensitive or classified information cleared, sanitized, or destroyed when no longer needed?	I			
6.	Are there mechanisms and procedures to downgrade media?	I			
7.	After declassification, are all of the classification and/or special handling labels removed from the system/media?	I			

Notes:
*** T = Test; A = Analysis; I = Inspection; D = Demonstration**
**** All "No" results should be accompanied by a written explanation.**

Supplemental Checklist Items

#	Test	Test Method	Yes	No	N/A
Application Program Controls					
1.	Have procedures been established to evaluate, test, and validate an application prior to placing it, or any changes to it, into operational or production status? a) Is the evaluation conducted by personnel not associated with the development group?	D			
2.	Are effective policies in place to ensure that once the information system(s) is accredited, add-on software is certified before being installed on the operational system?	D			
3.	Is DAA approval required for use of site-unique patches? Are such patches evaluated for their impact on the security of the system?	I			
4.	Are required security countermeasures (i.e., patches, etc.) implemented to correct known vulnerabilities? (AFCERT Advisories, ASSIST/CERT Bulletins) a) Have the following tests been performed, where applicable? (ref: CSET at AFCERT	T			
5.	Are system and application files protected from unauthorized deletion?	T			
Account Management					
6.	Does each user have his/her own account?	I			
7.	Does each administrators have his/her own account?	I			
8.	Are users locked out after 3 failed log-on attempts?	T			
9.	Are procedures in place to remove user names, passwords, and privileges of users who no longer require access to your system/network (i.e. For users who PCS, PCA, etc.)?	D			
10.	Users are prevented from gaining access to the network operating system from applications	T			
11.	Users can determine who will have access to their files	T			
12.	The administrator can produce a current list of all users and their access levels	I			
13.	The system permits all users to send files to a given user's area, but not read the other files that are located there or over-write them	T			
Administrative					
14.	Has an ISSO been designated for each information system?	I			
15.	Is the ISSO familiar with his/her duties?	I			
16.	Has the ISSO developed a system security policy for the system/network?	I			
17.	Does the system/network comply with the system security policy?	T			
18.	Has the ISSO developed and implemented procedures for handling of security incidents?	I			
19.	Are there procedures in place for the destruction/disposition of all hardcopy documents that contain sensitive unclassified and classified information?	I			
20.	Are terminals and surrounding areas examined often to detect passwords carelessly left about?	I			
21.	Are all personnel who handle, courier, process, or store sensitive or classified data aware of their responsibilities?	D			

22.	Is the proper documentation accomplished for all couriers?	I			
23.	Are there procedures established to ensure that all electronic information/data (i.e., documents, programs, scripts, patches, etc.) received is from a verified source and is valid (e.g., authentic, has not been tampered with, does not contain malicious code, etc.)?	I			
24.	Are authorized destruction methods (shredding, pulping, etc.) used to dispose of all hardcopy classified and/or sensitive but unclassified documents? a) If so, is the destruction device located in a controlled area?	I			
25.	Is the ISSO aware of his/her responsibilities and knowledgeable of the security policies, directives, and procedures?	D			
26.	Does the ISSO control the creation, distribution, and maintenance of passwords, keywords, or other similar access control codes?	I			
27.	Has the ISSO developed security incident response procedures?	I			
28.	Are procedures in place to report security incidents that could degrade the system security?	I			
29.	Are procedures in place to halt operations (when applicable) during a suspected security incident or as directed by a higher authority?	I			
30.	Is documentation detailing the system's hardware/ software configuration and the security measures that protect it maintained?	I			
31.	Are random checks conducted to ensure that security procedures and requirements established for the facility are being complied with?	I			
32.	Has the ISSO been specifically trained in the security features of the system?	I			
33.	Do manual procedures exist outside of the information system for the ISSO to upgrade, downgrade, or sanitize information? *(If so, describe how they are documented and enforced?)*	I			
Configuration/Change Control					
34.	Before granting other systems access/ connectivity to your system, you verify these systems have a current accreditation?	I			
35.	Are Memorandums of agreements accomplished with all outside organizations connected to this one?	I			
36.	Users cannot access the network operating system during login	T			
37.	Does the network operating system comply with 'object reuse'?	T			
38.	Are critical server configurations backed up and kept current?	T			
39.	Can users access the network operating system after login?	T			
40.	Do procedures exist for controlling the introduction of computer equipment, media, and software into the facility?	I			
41.	Are locally approved modifications to the system documented in detail and verified by the ISSO and other designated representatives?	I			

42.	Are programming changes and maintenance well controlled and documented for configuration management?	I			
43.	Is there a configuration inventory of all hardware, software, and documentation in the system/architecture? a) Does it include model variant numbers, serial numbers, etc.?	I			
44.	Are effective procedures implemented to inspect software and data files for malicious code prior to its installation or use?	T			
45.	Are effective procedures implemented to search for and remove malicious code from the system?	T			
46.	Is the ISSO informed of changes to the system prior to their installation?	I			
47.	Has the ISSO developed and implemented procedures to keep unauthorized hardware, software, and firmware off the system?	I			
48.	Have procedures been implemented to ensure the correct versions of the hardware, software, firmware, and documentation are installed/available?	I			
49.	Are backup copies of the applications software, operating system, and system utilities maintained and protected from destruction and/or tampering?	I			
System Access Controls					
50.	Is a list of all personnel granted access to the system maintained and is it periodically compared with the actual usage listings to identify any unexplained changes or discrepancies?	I			
51.	Is a software system used to check the sensitivity level of data accessed by user programs?	I			
52.	Is access to data files controlled by: a) The various levels and/or categories of data sensitivity? b) Logical portions within a file (i.e., block, record, field, or character) c) Specific permissions (i.e., read only, write only, append, etc.)?	T			
53.	Is there software protection (i.e., identification/authentication and audit) for the on-line operating systems, COTS products, and applications programs?	I			
54.	Are the privileges to add, delete, or modify files limited by software controls?	T			
55.	Does the system software restrict individual access to only the files for which the user is authorized?	T			
56.	Is access restricted to data, programs, and software systems on a need-to-know basis?	I			
57.	Are the access restrictions, if any, extended to copies in off-site storage?	I			
58.	Is access to password files severely restricted?	T			
59.	Is there an effective policy in place that requires users to logoff/disconnect their terminals from the system when they leave the vicinity of their terminals or during periods of inactivity?	I			
60.	Are factory-installed accounts, privileges, and passwords deleted when the system is installed?	T			
61.	Is there a means to ensure that only persons having the proper clearances and the need to know are given file access permission?	D			

62.	Is the need for user access to the computer systems and information revalidated periodically (e.g., annually) for users at the central site and all remote facilities?	I			
63.	Is the need for access to the network and network information, as well as network access, revalidated periodically for users at the central site and all remote facilities?	I			
64.	Are precautions taken to prevent loss of data from volatile memory during power interruptions (e.g., use of uninterrupted power supplies or emergency power generators)?	I			
65.	Is knowledge of and access to systems supporting special category information specifically granted on a need-to-know basis (i.e., formal access approval)?	I			
66.	Is removable magnetic media always kept in a closed container when not actually mounted in a disk drive?	I			
Remote Terminal Controls					
67.	Does the ISSO maintain liaison with remote facilities served by the system to ensure that terminal area security officers (TASOs) are assigned in writing?	I			
68.	Is an approved identification & authentication method employed for remote access protection to the system?	I			
69.	If passwords are used as the authentication method, do adequate procedures exist for establishing, distributing, and storing passwords for the remote users? a) Are they changed quarterly? b) Are passwords changed globally at random intervals?	D			
70.	Are remote terminal users restricted from access to source code to prevent possible overriding or altering of the operating system, security features, or system tables? a) Does the system allow for remote terminal system-level access? b) Are the system utility tools executable from any remote terminal stations?	T			
71.	Is access to all remote terminals controlled by: a) Locking doors? b) Guarded checkpoints? c) Other physical constraints?	T			
72.	Are the remote terminals themselves lockable? a) If so, are the keys positively controlled? b) Are the locks changed when keys are lost or stolen? c) If combination locks are used, are they changed periodically and upon the termination/ d) Reassignment of personnel?	T			
73.	Are the remote terminals located so that the privacy of each user is assured?	D			
74.	Are all remote terminals and the area immediately surrounding them protected at the highest sensitivity level of all data that the central system is processing online while the remote terminal is connected?	D			
75.	Do servers managing remote terminal access invoke automatic log-out for idle time?	T			
76.	Do remote terminals invoke a screen saver for idle time? a) If remote terminals have paging, do policies and procedures exist regarding page erasing prior to logout?	T			

77.	Do all communications links between system components meet the requirements for the transmission of the highest sensitivity/criticality level of information that can be accessed by any component?	I			
78.	Are all remote terminals restricted to a uniquely identified communications line or terminal identifier?	T			
79.	Are procedures available for the selective disconnection of the communications ports?	I			
Communications Security (COMSEC)					
80.	Has a COMSEC custodian been appointed?	I			
81.	Has a key management program been established?	I			
82.	Have procedures been established for destruction/safeguarding of COMSEC materials if the facility must be evacuated?	I			
83.	Are NSA-approved encryption devices used on all communication lines to protect classified information?	I			
84.	Are approved encryption devices/methods used on all communications lines to protect sensitive information?	I			
85.	Are wireless LANs encrypted with the appropriate encryption technology?	I			
86.	Is appropriate keying material available?	I			
87.	Was equipment installation in accordance with applicable requirements and guidelines?	I			
88.	Are procedures in place to negotiate COMSEC measures for the transit of information between the system and any separately accredited information systems? Are COMSEC measures documented in MOAs covering the interconnection and will they be implemented before the connection takes place?	I			
89.	Does the system authenticate the source of data?	I			
Auditing					
90.	Does audit reporting occur on the system?	D			
91.	Are audit reports reviewed at least weekly?	I			
92.	Are there in-place procedure for reporting incidents?	I			
93.	Are audit reports protected from tampering?	I			
Contingency and Emergency Planning/ Continuity of Operation					
94.	Are backups performed periodically?	I			
95.	Are backups stored off-site?	I			
96.	Is there a contingency plan for the system?	I			
97.	Are users trained on data backup procedures?	I			
98.	Are contingency plans reviewed at least annually?	I			
99.	Has the contingency plan successfully been tested in the past year?	I			
100.	Is the contingency plan periodically reviewed and updated?	I			
101.	Does the contingency plan address fire, flood, civil disorder, natural disaster, and bomb threat?	I			
102.	Is emergency lighting installed? Is it periodically tested?	I			
103.	Are emergency exits clearly marked?	I			
104.	Is the system free of overhead steam or water pipes (other than for fire suppression)?	I			
105.	Has a complete data backup plan been formulated and is it updated frequently?	I			
106.	Do data backups occur routinely for essential user data?	I			

107.	Is the backup data protected from destruction and/or tampering?	I			
108.	Are data backup procedures in place and tested to conduct essential system tasks after a disruption to the primary facility/system?	I			
109.	Are recovery procedures in place and tested to permit rapid restoration of the system following a disruption to the primary facility/system?	I			
110.	Has an alternate site been identified with compatible equipment?	I			
111.	Has the alternate site been tested during the past year?	I			
112.	Is surge protection installed for each piece of hardware?	I			
Firewalls					
113.	Is firewall configured to examine all incoming packets?				
114.	Is firewall configured to examine all outgoing packets?				
115.	Are all incoming attempts authenticated?				
116.	Are all unauthorized services blocked?				
117.	Which of the following protocols are authorized? FTP? HTTP? IPX? MIME? UDP? SMTP? TELNET? NFS? rlogin? rsh? RPC-based protocols?				
118.	Are all incoming connection attempts authenticated?				
119.	Is auditing enabled?				
120.	Are audits reviewed?				
Routers					
121.	Is remote configuring & monitoring via HTTP restricted per IP address?				
122.	Is strong authentication/passwords utilized?				
123.	Are access lists utilized?				
124.	Is "enable secret" password utilized?				
125.	Are access logs maintained?				
126.	Are logins via unencrypted protocol over untrusted networks authorized?				
127.	Is interactive access via Internet authorized?				
128.	Are anti-spoofing techniques utilized? (e.g. encryption)				
129.	Are unnecessary services (TCP, UDP, etc) disabled?				
130.	Are procedures in place to identify and block malicious IP addresses?				
Virtual Private Networks					
131.	Are filters utilized within tunnels?				
132.	Are digital signatures utilized?				
133.	Is strong encryption utilized?				

Notes:
* T = Test; A = Analysis; I = Inspection; D = Demonstration
** All "No" results should be accompanied by a written explanation.

ENCLOSURE C

TEST & CERTIFICATION TOOLS FOR OPERATIONAL CERTIFICATION OF SYSTEM ARCHITECTURE

1. Tools for Verification of System Architecture.

   a. MNS

      (1) Multi-Network Scanner v.91

      (2) Vulnerability scanner runs on Linux platform - includes cgi, qpop, sendmail, imap, named, ftp, and rpc scanners. Author homepage does not currently contain this software.

   b. Nmap

      (1) Nmap 2.3 (freeware UNIX network mapping www.insecure.org

      (2) Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques (determine what services the hosts are offering), and TCP/IP fingerprinting (remote host operating system identification). Nmap also offers flexible target and port specification, decoy scanning, determination of TCP sequence predictability characteristics, sunRPC scanning, reverse-identd scanning, and more.

2. Tools for Verification of Information Assurance.

   a. CyberCop

      (1) Network Associates CyberCop (NT Vulnerability Assessment)

      (2) CyberCop is an NT based Vulnerability Assessment tool that individually tests for various vulnerabilities on the network. It operates as host-based, meaning it tests every node on the network for individual weaknesses. It has additional features, which allow for network mapping.

   b. Hping

      (1) Hping 2 – beta 53 (freeware UNIX based Vulnerability Assessment)

      (2) Hping2 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. Hping2 handles fragmentation, arbitrary packet body and size and can be used in order to transfer files under supported protocols. Using hping2 you are able at least to perform the following jobs. Test firewall rules - [spoofed] port scanning - Test net performance using different protocols, packet size, TOS (type of service) and fragmentation. - Path MTU discovery - File transfer even between really fascist firewall rules. – Traceroute functionality under different

© SANS Institute 2000 - 2005 Author retains full rights.

protocols. - Firewalk like usage. - Remote OS fingerprint. - TCP/IP stack auditing.

c. Internet Scanner

(1) Internet Security Systems Internet Scanner

(2) Internet Scanner™ provides ongoing and decision-support reporting focused on the most critical aspect of managing risk by identifying and addressing network vulnerabilities. Performing scheduled and selective probes of communication services, operating systems, key applications, and routers, Internet Scanner uncovers the most comprehensive set of vulnerabilities most likely to be exploited during attempts to breach or attack your network and provides the necessary corrective action. Internet Scanner also provides trend analyses, conditional and configuration reports, and data sets to support sound, knowledge-based decision-making.

d. L0ftcrack

(1) L0ft Heavy Industries L0ftcrack (NT password cracking utility)

(2) This utility simply checks for the validity, integrity, and strength of passwords by using brute-force attack.

e. Satan

(1) Satan

(2) The original VA utility that is UNIX based. This tool is somewhat outdated, but can help identify some of the older vulnerabilities.

© SANS Institute 2000 - 2005 Author retains full rights.

ENCLOSURE D

TEST & CERTIFICATION REPORT

1. Executive Summary

2. Assumptions, Constraints, and Dependencies

3. Test Execution Log
   - 3.1 Time & Place of Test
   - 3.2 Configurations

4. Personnel Conducting Tests

5. Anomalies, Impromptu Tests, and Deviations
   - 5.1 Rationale
   - 5.2 Impact of Deviations on Test Results

6. T&C Findings
   - 6.1 Finding #1:
   - 6.2 Vulnerability Identification
   - 6.3 Potential Impact on Security of System
   - 6.4 Recommended Countermeasure(s) and Evaluation of Effectiveness of Proposed Countermeasure(s)
   - 6.5 (Note: For each finding, repeat the above four sub-paragraphs)

7. Conclusions and Recommendations:
   - 7.1 Conclusions
   - 7.2 Recommendations