Global Information Assurance Certification Paper

Diane Rojas
Security Essentials GSEC Practical Assignment
Version 1.2f

Accrediting National Security Systems

Introduction

In December, a federal judge ordered the Department of Interior (DOI) to shut down all connections to the Internet.[1] As of January 4, 2002 connections to the outside world via e-mail or Internet do not exist. According to a USA Today article[2], students can no longer search the US Fish and Wildlife database on endangered species, Park Service employees process timesheets by hand and mail them manually, permits for drilling can no longer be submitted electronically and DOI is facing other significant difficulties.

How could a federal court take such broad steps? It starts with the Computer Security Act of 1987[3], which established security standards for Federal computer systems. President Bush went one step further and established the National Security Telecommunications and Information Systems Security Committee (NSTISSC). However, The DOI failed to follow either's policies and the result was a complete shutdown of network operations.

The NSTISSC states that they provide "a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems through the NSTISSC Issuance System"[4]. They were tasked with providing guidance for accreditation and the result was the National Information Assurance Certification and Accreditation Process (NIACAP aka NSTISSI NO. 1000) available at http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf .

What is it?

It was written to be a guide to simplify the accreditation process. The NIACAP is a standard process that can be used to certify and accredit any of the systems that come under Office of Management and Budget (OMB) Circular A-130, Appendix III[5]. Since systems have a lifecycle, it was written to be flexible enough to allow for system growth and development.

How does an entity's system become accredited?

While NIACAP approaches accreditation and certification from a holistic perspective, this paper will concentrate on what is expected from the entities that wish to be granted accreditation. It also tries to address the obstacles to certification inherent in small government offices and offers solutions. In addition, I have clarified some of the language in the document and provided additional resource links for those seeking accreditation.

Dissecting the NIACAP

For simplicity's sake I will refer to the entity as a department. In actuality this can be as large as a department or as small as an individual office. Each level of a government entity would have a separate certification and accreditation.

First, the department must decide who will be working on this project. The NIACAP defines three roles for the department along with a third-party certifier who will conduct the certification.

The three roles that the department must provide are the program manager, Designated Approving Authority (DAA), and user representative[6]. The guidelines indicate that the certification process have three roles. Smaller offices may have trouble finding the exact person to fit each of these roles.

Because of government hiring freezes and typical low salaries in government technical fields, techs and engineers are in short supply on the government side. This can lead to an information security vacuum in IT. The program manager should be an IT manager or a system administrator with sufficient project management capability. He will have to manage not only the security aspects of IT but also budgeting of equipment, systems operation and performance and other related responsibilities[7].

The DAA should have budgetary and business knowledge with the authority to sign off on the security measures[8]. Very often DAAs are not aware of the more technical aspects of security and they should work closely with the security officer and/or systems administrator to address those deficiencies.

Although the NIACAP does not require an Information Systems Security Officer (ISSO), based on my experience, it can be more useful to include this function during development rather than once the system is in operation. An ISSO should be able to supply insight because his job function requires he deal with these issues on a daily basis as opposed to a strictly technical or administrative position.

In some smaller entities the role of the Information Systems Security Officer (ISSO) and the system administrator are one and the same, since ISSO can be a collateral duty. The ISSO can also be an administrator with very little technical knowledge. In these situations one must use common sense to cover all the bases. Consult with IT staff or hire a third-party contractor if needed.

The user representative role is also important. While there can be a tendency to ignore user complaints, one must not inhibit productivity in the workplace with overly stringent and counterproductive security requirements. The employees using the system have a better understanding of their everyday needs, which should be balanced carefully with security measures.

While the program manager coordinates, the DAA, certifier and user representative provide useful information and support.[9]

Now that we have a committee, what will it be doing? It will develop and establish a System Security Authorization Agreement (SSAA). This is a baseline necessary for operation, before development or changes to a system[10]. It is a collection of documents that summarize all the security requirements and solutions for accreditation.

The NIACAP lists 3 types of accreditation: System, Site and Type. A system accreditation is fairly straightforward since it deals with a single general support system or major application. A site accreditation addresses all the applications and systems at a particular location. Departments that have multiple locations and distributed applications use a type accreditation[11]. This is more cost effective, because identical copies of a system can be deployed and the local operators take on the responsibility for compliance with the SSAA, without each site having to be accredited separately[12].

The NIACAP defines four phases of accreditation: Definition, Verification, Validation and Post Accreditation.[13]

The Definition phase, Phase 1, consists of collecting documentation from your organization and basic security planning. At this point the NIACAP instructs you to choose a level of certification. However these levels are not defined anywhere. Apparently they will be published by the NSTISSC in a separate document called the Implementation Manual at some point[14]. In the meantime we can use the guidance from the Computer Security Act of 1987, which states that standards imposed cannot "adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings[15]." Adequate security is also defined in the Appendix III to OMB Circular No. A-130 as being "security commensurate with the risk and magnitude of harm" provided "through the use of cost effective management, personnel, operational and technical controls.[16]"

If you still find you need more guidance you can look to the Common Criteria found at http://csrc.nist.gov/cc/ccv20/ccv2list.htm or to NIST's library of security guidelines at http://www.itl.nist.gov/fipspubs/0-toc.htm#cs . Some of these are the NIST 800-26, Security Self-Assessment Guide for Information Technology Systems and the NIST 800-12 An Introduction to Computer Security: The NIST Handbook and NIST 800-18 Guide for Developing Security Plans for Information Technology Systems. NIST will also be publishing new guides this year. Additional information can be found at Federal Computer Week's site, http://www.fcw.com/fcw/articles/2002/0128/web-nist-01-28-02.asp [17].

First you will need to determine your department's security budget and define the boundaries of the accreditation. Collect any existing documentation on your system such as system design documents, standard operating procedures, user manuals, any previous security plans, risk analyses and contingency plans[18]. And remember to get any guidance documents that pertain to your department specifically. For instance, the Department of Interior itself should have a guide

for security planning that promotes uniformity among its individual divisions and offices. This saves valuable time on repetitive tasks and documentation.

The next task is to meet and start writing the SSAA. A list of documents and the SSAA format you will need is provided in the Annex A to the NIACAP. As this is only the first run of SSAA, all the documents may not be completed at this stage[19]. This is because the security testing does not take place until Phase 3, Validation, and the evaluations have not yet been generated.

When the DAA determines that all IA requirements are included, the certifier evaluates the security features against the security requirements taking into consideration cost and feasibility, the program manager reviews for accuracy, cost and scheduling, and the user representative determines that it will support the users mission then the baseline is drawn up[20]. Your SSAA is now defined.

Phase 2 is Verification. It consists of developing a system or modifications to a system and then addressing any new vulnerabilities that arise[21]. Established systems that are not going through major changes do not have to address this. For those that are designing and developing new systems, those documents related to the changes such as system design documents, new software integration, new network architecture document should be collected[22]. Test plans and procedures for systems functionality requirements must be written and conducted[23]. A vulnerability assessment and a statement of residual risk must be prepared[24]. Any major security problems identified would require returning to Phase 1 to address the matter before moving forward[25]. If your results are acceptable, move on to Phase 3[26].

In Phase 3, Validation, all the work completed in Phases 1 and 2 are validated. The certifier conducts a Security Test and Evaluation (ST&E)[27]. Other testing such as penetration testing, TEMPEST Verification and validation of COMSEC compliance may be done[28]. Your system must comply with Federal Regulations, any requirements of the Department and other restrictions as appropriate to the level of security. All documents in the SSAA will be evaluated, contingency plans, configuration management[29]. A security test report will be generated and a recommendation given to the DAA as to whether or not to certify the system[30]. Once the DAA receives this recommendation, a determination is made as to whether the system should be accredited[31].

"If the decision is to accredit, the decision must include the security parameters under which the information system is authorized to operate[32]." If the system is denied accreditation, an Interim Approval to Operate (IATO) can be given to mission critical systems with an agreement to implement proposed solutions, schedule and an expiration date. If the DAA decides not to grant an IATO, you must return to Phase 1 and agree to an acceptable level of risk. The DAA must give a reason and if possible solutions[33].

Phase 4 concerns ongoing maintenance to the security system and security operations. It stops only when a new or largely revised version of the SSAA is needed.[34] The ISSO is responsible for requesting approval for changes and for the documenting of those changes[35]. Approval is obtained from all the persons previously involved[36] or their replacements.

Periodic evaluations of the SSAA, the physical, personnel and management control, COMSEC evaluation, contingency plan, change management, systems security management and risk management are necessary. Mandatory periods of recertification and reaccredidation are at minimum every three years in accordance with OMB Circular A-130, Appendix III[37]. The DAA, user representative, program manager and the certifier agree on a shorter period for internal reviews and document it in the SSAA[38].

Be careful when reading paragraph 35a(4) of the NIACAP. While the heading says Compliance Evaluation, the diagram states COMSEC evaluation. That paragraph then goes on to describe COMSEC evaluation, which analyzes whether or not the communications security requirements are integrated into the systems architecture and site management procedures.

The NIACAP specifies the User Representative to report vulnerabilities and security incidents. These would then be recorded and acted upon by the ISSO. Any changes to the SSAA requested by the ISSO based on these incidents are subsequently approved by the DAA, user representative and program manager[39].

Remember to keep contact information in contingency plans current. Any time there is a personnel change that affects the contact list it should be reported to the ISSO and documented in the SSAA[40].

Compliance validation is also part of Phase 4. It is a repeat of all the applicable Phase 2 and 3 tasks plus these following minimum tasks: [41]

Site and Physical Security Validation
Security Procedures Validation
System Changes and Related Impact Validation
System Architecture and System Interfaces Validation
Management Procedures Validation
Risk Decisions Validation.

These are the minimum activities for Phase 4[42]. These are not defined anywhere in the document however, referring to the SSAA and comparing it to these issues would be a valid evaluation. Anything found to be inconsistent would need to be addressed and the SSAA updated.

When the IATO expires or if an SSAA is no longer valid the DAA will terminate operations. This would require a return to Phase 1 to write a new or updated SSAA[43].

In conclusion, the NIACAP identifies and reinforces a certain set of standards and guidelines used to formulate a stringent but flexible set of accreditation procedures. The methodology incorporates a four-phase plan that includes defining the systemic vulnerabilities in security within the organization through a thorough and comprehensive risk assessment; using this assessment to identify the level of accreditation required; verifying that there are no changes to the original assessment and formulating test plans and procedures for system functionality; ensuring that the solutions are validated through system test and evaluation; and finally implementing the security process into the system life cycle.

In addition to the four-phase approach, there were several recommendations made that can be implemented to provide further clarification of the accreditation process. These include the review of NIST and Common Criteria security guidelines, adding the ISSO to the four defined roles, and the addition of a technical advisor skilled in IT security whose responsibility is to formulate recommendations for the non-technical ISSO. Further details are expected in the Implementation Manual from NSTISSC and the new NIST guidelines to be published in 2002.

1. Edward Walsh ,"Interior Dept. Blocks Web Access at Judge's Order", *Washington Post,* December 8, 2001; Page A04; http://www.washingtonpost.com/ac2/wp-dyn/A10955-2001Dec7?language=printer .

2. Tom Kenworthy, "Phone, fax will have to do for offline Interior Dept.; Web sites, Internet access suspended amid concerns over financial data security", *USA Today*; Jan 4, 2002;no longer available on the Web for free but is available through the USA Today archives website for a fee.

3. US Congress**,** Computer Security Act of 1987, Public Law 100-235,100th Congress, 1987; http://www.net.ohio-state.edu/hypertext/csa-1987.html .

4. NSTISSC website, overview, http://www.nstissc.gov/html/overview.html .

5. Office of Management and Budget, CIRCULAR NO. A-130, Revised, February 8, 1996; http://www.whitehouse.gov/omb/circulars/a130/a130.html .

6. Committee on National Security Systems, formerly National Security Telecommunications and Information Systems Security Committee (NSTISSC), *National Information Assurance Certification and Accreditation Process (NIACAP)*, April 2000, Paragraph 6

7. NIACAP, Paragraphs 7 and 46

8. NIACAP, Paragraph 7

9. NIACAP, Section 12

10. NIACAP, Section 4

11. NIACAP, Paragraph 9

12. NIACAP, Paragraph 32d

13. NIACAP, Paragraph 15

14. NIACAP, Paragraph 1

15. Computer Security Act of 1987, Section 4, (3)

16. OMB Circular A-130, Paragraph A.2.a

17. Diane Frank, "NIST Prepping Security Guides", *Federal Computer Week*, Jan. 28, 2002

18. NIACAP, Section 6

19. NIACAP, Section 6

20. NIACAP, Section 6

21. NIACAP, Section 7

22. NIACAP, Section 7

23. NIACAP, Section 7

24. NIACAP, Section 7

25. NIACAP, Section 12

26. NIACAP, Section 12

27. NIACAP, Section 8

28. NIACAP, Section 8

29. NIACAP, Section 8

30. NIACAP, Paragraph 31

31. NIACAP, Paragraph 32

32. NIACAP, Paragraph 32

33. NIACAP, Paragraph 32b

34. NIACAP, Section 9

35. NIACAP, Section 9

36. NIACAP, Section 9

37. OMB Circular A-130, Appendix III, Paragraph A3a(3)

38. NIACAP, Paragraph 36

39. NIACAP, Section 12

40. NIACAP, Page 35

41. NIACAP, Page 36

42. NIACAP, Page 36

43. NIACAP, Figure 6

References

1. Edward Walsh ,"Interior Dept. Blocks Web Access at Judge's Order", *Washington Post,* December 8, 2001

2. Tom Kenworthy, "Phone, fax will have to do for offline Interior Dept.; Web sites, Internet access suspended amid concerns over financial data security", *USA Today*; Jan 4, 2002

3. US Congress, Computer Security Act of 1987, Public Law 100-235,100th Congress, 1987;

4. Office of Management and Budget, CIRCULAR NO. A-130, Revised, February 8, 1996

5. Committee on National Security Systems, formerly National Security Telecommunications and Information Systems Security Committee (NSTISSC), *National Information Assurance Certification and Accreditation Process (NIACAP)*, April 2000