HCFA/Business Partners Security Oversight Manual

Department of Health and Human Services (DHHS)
HEALTH CARE FINANCING ADMINISTRATION (HCFA)

Transmittal 1 **Date: JANUARY 26, 2001**

CHANGE REQUEST 1439

CHAPTERS	REVISED SECTIONS	NEW SECTIONS	DELETED SECTIONS
1-3	---------	ALL	----------
Appendix A	---------	ALL	----------

NEW/REVISED MATERIAL--EFFECTIVE DATE: January 26, 2001
IMPLEMENTATION DATE: January 26, 2001

This transmittal replaces the following:

Regional Office Manual (ROM), Chapter III, Claims Process, Systems Security
- Section 3250 – Systems Security Authority
- Section 3251 – RO Responsibilities
- Section 3252 – Provide Technical Guidance
- Section 3253 – Monitor Compliance
- Section 3254 – Report To BPO
- Section 3255 – Coordinate External Systems Security Audits
- Section 3256 – Special Budget Requests
- Section 3257 – Schedule/Checklist Exhibits
  - Exhibit A – Medicare Risk Analysis Schedule
  - Exhibit B – Medicare Contingency Planning Schedule
  - Exhibit C – Medicare Risk Analysis Checklist
  - Exhibit D – Medicare Contingency Planning Checklist

Material in the above manual and associated sections/exhibits is being replaced in its entirety. A reference page in the ROM, Chapter III, Claims Process, Systems Security will now point to the recently developed HCFA/Business Partners Security Oversight Manual (a hyperlink will be provided). Consortium Contractor Management Officers (CCMOs), HCFA Project Officers (POs), and other security staff will now be required to follow the new IT systems security program management requirements when providing systems security oversight activities for HCFAs business partners.

MAJOR CHANGES

The security sections of the ROM identified above, have been updated and consolidated into a new manual called the **HCFA/Business Partners Security Oversight Manual**. The existing security sections in the ROM will be deleted. The new manual is comprised of the following sections:

- Chapter 1 – Introduction
  This chapter provides an overview of the HCFA/Business Partners Security Oversight Manual and references documents used to develop the manual, specifically Federal and HCFA mandates and guidelines for the handling and processing of Medicare data.

- Chapter 2 – IT Systems Security Roles and Responsibilities
  This chapter provides a description of the Consortium Contractor Management Officer (CCMO), the HCFA Project Officer (PO), Business Partners, Senior Information Systems Security Officer (SISSO), and the Component ISSOs (central and regional offices). The roles and responsibilities of these entities are described in detail.

- Chapter 3 – IT Systems Security Program Management
  This chapter contains a program management planning table that will assist CCMOs, POs, and other security staff in coordinating system security oversight activities at a business partner site.

- Appendix A: Audit Protocols and the Contractor Assessment Security Tool (CAST)
  This appendix provides procedures designed to verify that sites are in compliance with systems security requirements and a tool to assist business partners in performing required annual systems security self-assessments. The appendix also includes a hyperlink to an Adobe Acrobat (.pdf) file containing the HCFA Core Set of Security Requirements – Audit Protocols.

These instructions should be implemented as specified in Program Memorandum Intermediaries/Carriers, Change Request 1439.

Health Care Financing Administration (HCFA)
Business Partners
Security Oversight Manual

HEALTH CARE FINANCING ADMINISTRATION
SECURITY AND STANDARDS
7500 SECURITY BOULEVARD
BALTIMORE, MD 21244-1850

January 2001

HCFA/Business Partners Security Oversight Manual

Appendices

1. Introduction (Rev. 1 – 01-26-01)

The Health Care Financing Administration (HCFA) requires that its business partners implement Information Systems security controls in order to maintain the confidentiality, integrity, and availability of Medicare systems operations in the event of computer incidents or physical disasters.

A HCFA business partner is a corporation or organization that contracts with HCFA to process or support the processing of Medicare Fee-for-Service claims. These business partners include Medicare carriers, intermediaries, Common Working File (CWF) host sites, durable medical equipment regional carriers (DMERCs), standard claims processing system maintainers, regional laboratory carriers, and claims processing data centers.

This HCFA/Business Partners Security Oversight Manual was developed to provide guidance and reference for the Consortium Contractor Management Officer (CCMO) and the HCFA Project Officer (PO) in their role as security coordinator. It is designed to ensure that safeguards for the protection of the integrity, availability, and confidentiality of information technology (IT) resources (e.g. data, information, applications, and systems) are present at HCFA business partners facilities.

This manual includes the following:

- An overview of primary security roles and responsibilities (see Section 2)
- A program management schedule that will assist the Consortium Contractor Management Officer (CCMO), the Project Officer (PO), and other security staff in coordinating a system security program (see Section 3)
- Appendix A: HCFA Audit Protocols, provides an Internet link to an Adobe Acrobat (.pdf) file of the HCFA Core Security Requirements and Audit Protocols.
- A companion document, the HCFA Business Partners Systems Security Manual, includes security guidance information for use by HCFA business partners.

The HCFA IT systems security program and Core Security Requirements/Audit Protocols were developed in accordance with Federal and HCFA documents that mandate the handling and processing of Medicare data. These documents include the following:

- OMB Circular No. A-127, Financial Management Systems, February 8, 1996.
  http://www.whitehouse.gov/omb/circulars/a127/a127.html
- Presidential Decision Directive/NSC – 63 (PDD 63), May 22, 1998.
  URL to “White Paper: Clinton Administration’s Policy: Critical Infrastructure Protection”:
  http://www.whitehouse.gov/WH/EOP/NSC/html/documents/NSCDoc3.html
- Federal Information System Controls Audit Manual (FISCAM), GAO/AMID-12.19.6, Undated.
  http://www.gao.gov/special.pubs/12_19_6.pdf

- HCFA SSP Methodology.
  http://www.hcfa.gov
- IRS 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, Rev 3-99
  http://ftp.fedworld.gov/pub/irs-pdf/p1075.pdf
- Health Insurance Portability and Accountability Act (HIPAA), 1996.
  http://www.hcfa.gov/medicaid/hipaa/source/hipaasta.pdf
- HCFA Systems Security Policy Standards and Guidelines Handbook.
  http://www.hcfa.gov

Additional documents were used as references in the development of this manual and the HCFA Core Security Requirements. These documents include the following:

- Department of Health and Human Services, Automated Information Systems Security Program Handbook (DHHS AISSP).
  http://wwwoirm.nih.gov/policy/aissp.html
- NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability (CSIRC), November 1991.
  http://csrc.ncsl.nist.gov/nistpubs/800-3.pdf
- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, SP800-12.
  http://csrc.ncsl.nist.gov/nistpubs/800-12/
- National Archives and Records Administration Regulation 36 CFR Part 1228 Subpart K, NARA36
  http://www.nara.gov/nara/cfr/cfr1228k.html
- Code of Federal Regulations, (5 CFR) Part 731 – Suitability, 5CFR731
  http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html
- FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25 U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, PUB46-3.
  http://csrc.nist.gov/cryptval/des/fr990115.htm
- HCFA Internet Policy
  http://www.hcfa.gov/security/isecplcy.htm

These publications require HCFA business partners and their subcontractors to:

- Implement comprehensive systems security programs;
- Safeguard records against errors or improper disclosures that could cause beneficiaries substantial harm, embarrassment, inconvenience, or unfairness;
- Provide internal control review and prompt, efficient corrective actions;
- Train employees in security awareness and practices;

- Maintain workable business continuity and contingency plans; and
- Provide a Systems Security Officer (SSO) to manage the systems security program for Medicare operations and to assure that necessary safeguards are in place and working.

HCFA Core Security Requirements and Audit Protocols will be updated periodically to reflect changes in these or other applicable documents (e.g., publication of final HIPAA rule on IT systems security).

2. IT Systems Security Roles and Responsibilities (Rev. 1 -- 01-26-01)

Consortium Contractor Management Officers (CCMOs) are responsible for the oversight of Medicare carriers and intermediaries. HCFA Project Officers (PO) (generally located in central office business components) are responsible for the oversight of the other business partners. These include Common Working File (CWF) host sites, durable medical equipment regional carriers (DMERCs), standard claims processing system maintainers, regional laboratory carriers, and claims processing data centers.

2.1 Consortium Contractor Management Officer and HCFA Project Officer (CCMO/PO)

The CCMO and PO are responsible for security programs and have the following responsibilities:

- HCFA point of contact for business partners IT systems security problems and IT system security technical guidance.
- Central point for the reception from the business partners of security incident reports.
- CCMO reports security incidents to the Regional Information System Security Officer and the HCFA Action Desk at phone number (410) 786-2580. The Project Officer reports only to the HCFA Action Desk.
- Central point for the reception from the business partners for the reports and documentation identified in Table 3.1 shown in Section 3.
- Review and support resolution of business partners operational issues.
- The CCMO and PO will go to the HCFA central office for technical questions and issues.
- Provide technical guidance and/or assistance in response to business partner's requests. The CCMO and PO must know HCFA's core security requirements and the information in the Business Partners System Security Manual.
- Follow-up and document corrective actions taken as a result of SAS-70, OIG and Annual Compliance Audit reports. Ensure that all corrective action plans are implemented, whether they are SAS-70, CFO, or Annual Compliance Audit plans.
- Attend all audit entrance and exit conferences so that knowledgeable judgements about the appropriateness and potential effectiveness of the planned actions can be made.
- Assure the required security plan documentation is being developed and is receiving the appropriate contractor management attention and submitted in a timely manner.
- Monitor the self-assessment process, assuring that it is initiated and completely timely. Determine if the appropriate management attention is being devoted to the self-assessment and gap analysis processes. Assure the submitted CAST data is complete. A small number of CAST elements will be selected for quality review which the CCMO, PO and systems specialists will perform using developed protocols.

- Confirm that the annual internal system security compliance certification is submitted in a timely manner.
- Confirm that the Business Continuity and Contingency Plan is filed in a timely manner in the System Security Profile.
- Confirm that the triennial risk assessments are performed and reviewed annually. Work with the business partners to ensure that the scheduling of this important security activity does not conflict with other priorities, or get dropped.
- Provide recommendations to HCFA central office and regional budget staffs on system related budget requests submitted by the business partners during the year.
- Provide representatives for the Information Systems Security Technical Advisory Group meetings.

2.2 Business Partners

All business partners, subcontractors and their employees supporting HCFA are required to comply with the security requirements of HCFA IT systems security and all systems security related Federal statutes, regulations and policies.

Each HCFA business partner will designate a principal System Security Officer (SSO) who is responsible for planning and managing the system security program and assuring that necessary safeguards are in place and working. This officer must be organizationally independent of ADP operations. If additional security officers are needed at various organizational levels, their security actions are approved through the principal SSO.

2.3 Senior Information Systems Security Officer (SISSO)

The HCFA Senior Information Systems Security Officer (Senior ISSO) in the HCFA Office of Information Services (OIS) is responsible for the following:

- Ensuring that SSP are developed, reviewed, implemented, and revised for its internal systems.
- Ensuring that systems security risk assessments are developed, reviewed, and implemented for the SSP process for its internal systems.
- Reporting security incidents in accordance with the systems security incident reporting procedures developed and implemented by Federal mandates, DHHS, and HCFA policies for its internal systems.
- Assisting other ISSOs (central and regional offices) in developing local security procedures for either in place SSP or for those under active development.
- Researching state-of-the-art systems security technology and disseminating informational material in a timely fashion.
- Developing and implementing an IT security training and orientation program.

2.4 Component ISSO (Central and Regional Offices)

Designated by HCFA as the approving security officer authority for ensuring the security of a HCFA component's information system throughout its life cycle, from design through disposal.

Component ISSO (central and regional offices) responsibilities include:

- Ensure that the component's SSP is developed and implemented according to HCFA's IT systems security policies and procedures.
- Manage the assurance of systems security-related issues.
- Act as the primary point of contact for information security issues for its systems.

3. IT Systems Security Program Management (Rev. 1 -- 01-26-01)

Use the following table (Table 3.1) in planning reviews of deliverable reports and documents from the contractor. Remind the contractor of their due dates for the deliverables and validate that they have been received in a timely manner. The number accompanying each entry in the Requirement column indicates the section in the HCFA Business Partners System Security Manual that addresses that particular requirement.

Table 3.1 Planning Table

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
A-2 Self-Assessment using CAST	Each Federal fiscal year	CCMO/PO with a copy to HCFA CO Systems Security Profile	See Appendix A, Section A-2, for an overview of CAST. Self-assessment results recorded using CAST are to be included as part of the Certification Package.	
3.1 System Security Plans	Each Federal fiscal year for each GSS and MA, or upon significant change	Systems Security Profile	System Security Plans (SSP) are to be reviewed and updated as necessary and are to be included as part of the Certification Package. More information about System Security Planning can be found in the HCFA SSP Methodology.	
3.2 Risk Assessment (Report)	Every 3 years or upon significant change	Systems Security Profile	Risk Assessments are to be included as part of the Certification Package.	
3.3 Certification	Each Federal fiscal year	CCMO/PO with a copy to HCFA CO	Each year HCFA will issue a program memorandum (PM) on internal control certification. This PM will contain information on certification requirements including where, when, and to whom these certifications must be submitted.	

Requirement	Frequency	Send To	Comments	Complete (Check Box if Complete)
3.4 Business Continuity and Contingency Plan (Update)	Each Federal fiscal year, or upon significant change	Systems Security Profile	Management and the SSO must approve the Plan. Plans are to be included as part of the Certification Package. More information about contingency planning can be found in *An Introduction to Computer Security: The NIST Handbook* .	
3.5 Compliance	Each Federal Fiscal year	CCMO/PO with a copy to HCFA CO Systems Security Profile	There are two (2) components to compliance: **(1) Annual Compliance Audit:** Once a year, an annual compliance audit will be performed on four (4) categories of the HCFA Core Security Requirements to validate the self-assessment. HCFA will determine the four categories the audit will validate by way of a Program Memorandum (PM). **(2) Corrective Action Plan** Corrective Action Plans address findings of annual self-assessments. CAST (see Appendix A, Section A-2) will record all items assessed as “Partial” or “Planned”. The Corrective Action Plan is the set of all “Partial” and “Planned” items, along with their “Comments/Explanations” and “Projected Completion Dates.”	
3.6 Incident Reporting and Response	As necessary	CCMO/PO Systems Security Profile	The HIPAA also addresses Incident Reporting information.	
3.7 System Security Profile	As necessary	On file in the Security organization	See HCFA SSP Methodology for additional information on the System Security Profile.	

LEGEND:

Contractor Assessment Security Tool	CAST
Central Office (HCFA)	CO

Consortium Contractor Management Officer	CCMO
Senior Information Systems Security Officer (HCFA)	SISSO
Business Partners Systems Security Officer	SSO
Project Officer (HCFA)	PO
General Support System	GSS
Major Application	MA

The CAST tool and associated audit protocols are available to the CCMO/PO to assist in reviewing the business partner's security program. The CCMO/PO will use CAST for assessing reports on each business partner Corrective Action Plan. The CCMO/PO will also be able to review the thoroughness or completeness of the Annual Self-assessment by checking a random sample of responses to the HCFA Core Security Requirements. See Appendix A for the Audit Protocols and additional information on the CAST.

Appendix A: Audit Protocols and the Contractor Assessment Security Tool (CAST)

A-1 Audit Protocols (Rev. 1 -- 01-26-01)

HCFA has developed Core Security Requirements to detail technical requirements for business partners who use IT systems to process Medicare data. Business partners must establish and maintain responsible and appropriate safeguards to ensure the confidentiality, integrity, and availability of Medicare data.

Audit Protocols are recommended self-assessment procedures designed to verify that sites are in compliance with system security requirements. Protocols are not security requirements; rather, they have been developed based on the same Federal and HCFA security documents used to create the HCFA Core Security Requirements (see Appendix A of the HCFA/Business Partners Systems Security Manual).

The Contractor Assessment Security Tool (CAST) will assist business partners in performing required annual systems security self-assessments and will also assist them in preparing for periodic audits by agencies, such as the Government Accounting Office (GAO), Internal Revenue Service (IRS), DHHS Office of Inspector General (OIG), and HCFA.

HCFA has organized the Core Security Requirements into Categories, General Requirements, Control Techniques, and Protocols. There are ten Categories comprised of six general Categories, three application Categories, and an additional Category, “Networks.” The ten categories are as follows:

Category	Description
Entity-wide Security Program Planning and Management Elements	These controls address the planning and management of an entity's control structure.
Access Control	These controls provide reasonable assurance that information-handling resources are protected against unauthorized loss, modification, disclosure or damage. These controls are logical and physical.
System Software	These controls address access and modification of system software. System software is vulnerable to unauthorized change and this category contains critical elements necessary for providing needed protection.
Segregation of Duties	These controls describe how work responsibilities should be segregated so that one person does not have access to or control over all of the critical stages of an information handling process.
Service Continuity	These controls address the means by which the entity attempts to ensure continuity of service. A business partner cannot lose its capability to process, handle, and protect the information it is entrusted with.

Category	Description
Application Software Development and Change Control	These controls address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information.
Application System Authorization Controls	These controls address the processing of Medicare data in a manner that ensures that only authorized transactions are entered into the information processing system.
Application System Completeness Controls	These controls ensure that all system transactions are processed and that any missing or duplicate transactions are identified and a remedy implemented.
Application System Accuracy Controls	These controls address the accuracy of all data entered into systems for processing, handing, and storage. Data must be valid and accurate. All invalid, erroneous, or inaccurate data must be identified and corrected.
Networks	These controls address the network structure. The network structure must be protected and the data transmitted on the networks must be protected.

Each category is further organized into General Requirements, Control Techniques, and Protocols. Figure A-1 below shows the relationship between General Requirements, Control Techniques, and Protocols.

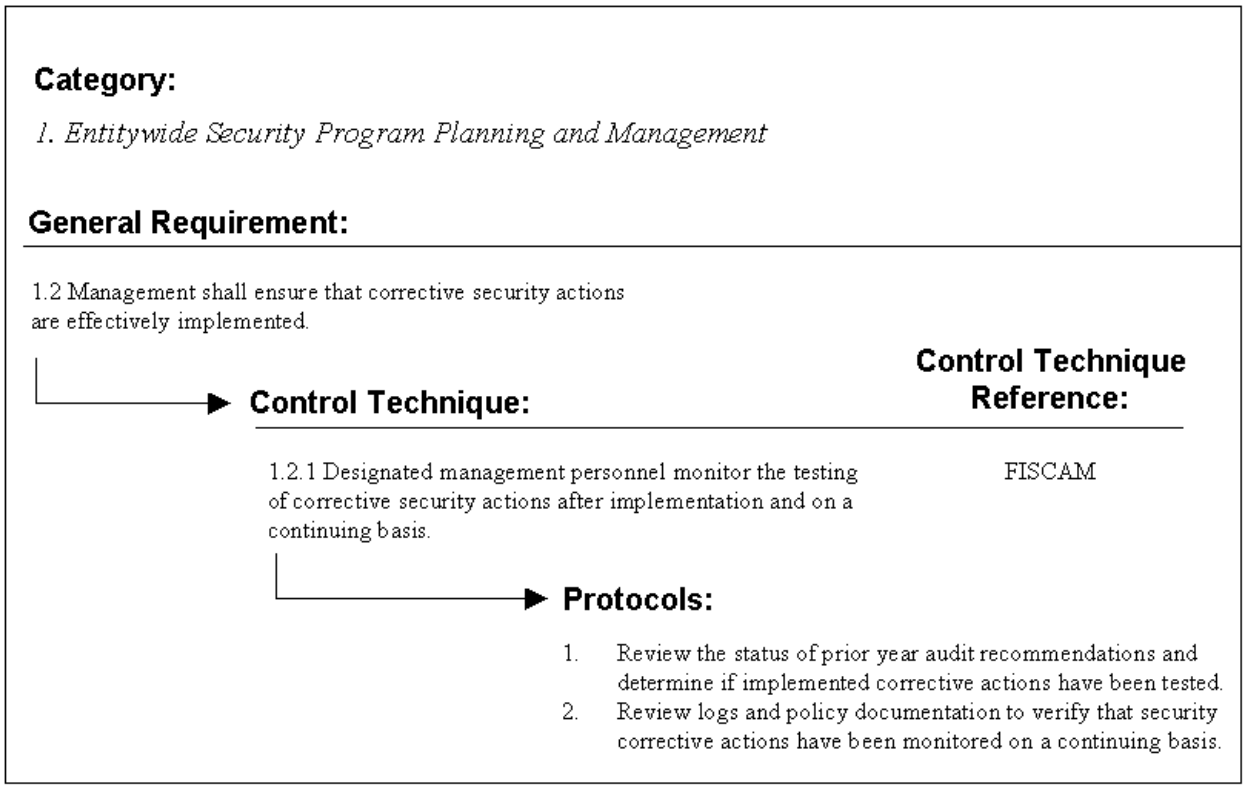

Figure A-1. Relationship between General Requirements, Control Techniques, and Protocols

General Requirements define elements of systems or operations that must be safeguarded. The example above shows General Requirement 1.2 from the Category "Entitywide Security Program Planning and Management." The General Requirement states that "Management shall ensure that corrective security actions are effectively implemented."

Control Techniques describe particular system elements that must be in place to consider the General Requirement valid. The example above shows Control Technique 1.2.1, which states that "Designated management personnel monitor the testing of corrective security actions after implementation and on a continuing basis." A business partner would be in compliance with General Requirement 1.2 if Control Technique 1.2.1 has been validated. To assist in this validation, HCFA has developed Audit Protocols.

Click the hyperlink below to download a copy of the Audit Protocols in Adobe Acrobat (.pdf) format.

[Inset hyperlink to Audit Protocols.pdf]

A-2 The Contractor Assessment Security Tool (CAST) (Rev. 1 -- 01-26-01)

HCFA provides its business partners with CAST. CAST is an automated database and software application that enables business partners to perform their self-assessments by entering data into electronic CAST forms that include the HCFA Core Security Requirements and Protocols. The HCFA business partner will provide the CAST output as part of submitted certification material.

CAST provides business partners with a powerful reporting tool that generates formatted self-assessment forms, copies of HCFA Core Security Requirements, and standardized site-analysis reports. CAST also records information about a site, Risk Analysis schedules, and Contingency Planning schedules.

HCFA business partners can use the CAST Q&A form (Figure A-2 below) to conduct automated self-assessments. The CAST database includes Protocols designed to assess compliance with Core Security Requirements. HCFA requires that business partners complete annual self-assessments using CAST. The self-assessment will be included in the Security Profile (Section 3.7 of the HCFA business Partners Systems Security Manual). Business partners can also use CAST to conduct self-assessments in preparation for audits by specific external agencies. CAST allows the business partner to generate a Q&A form that consists of those Core Security Requirements and Protocols that have a particular source document as a reference (e.g., IRS 1075, GAO FISCAM).

When entering information into CAST, the business partner will provide specific information in the Explanation/Comment field as to how they meet the requirement. CAST can then produce a formatted report of self-assessment results. CAST can also be used to analyze security data and output graphical analyses.

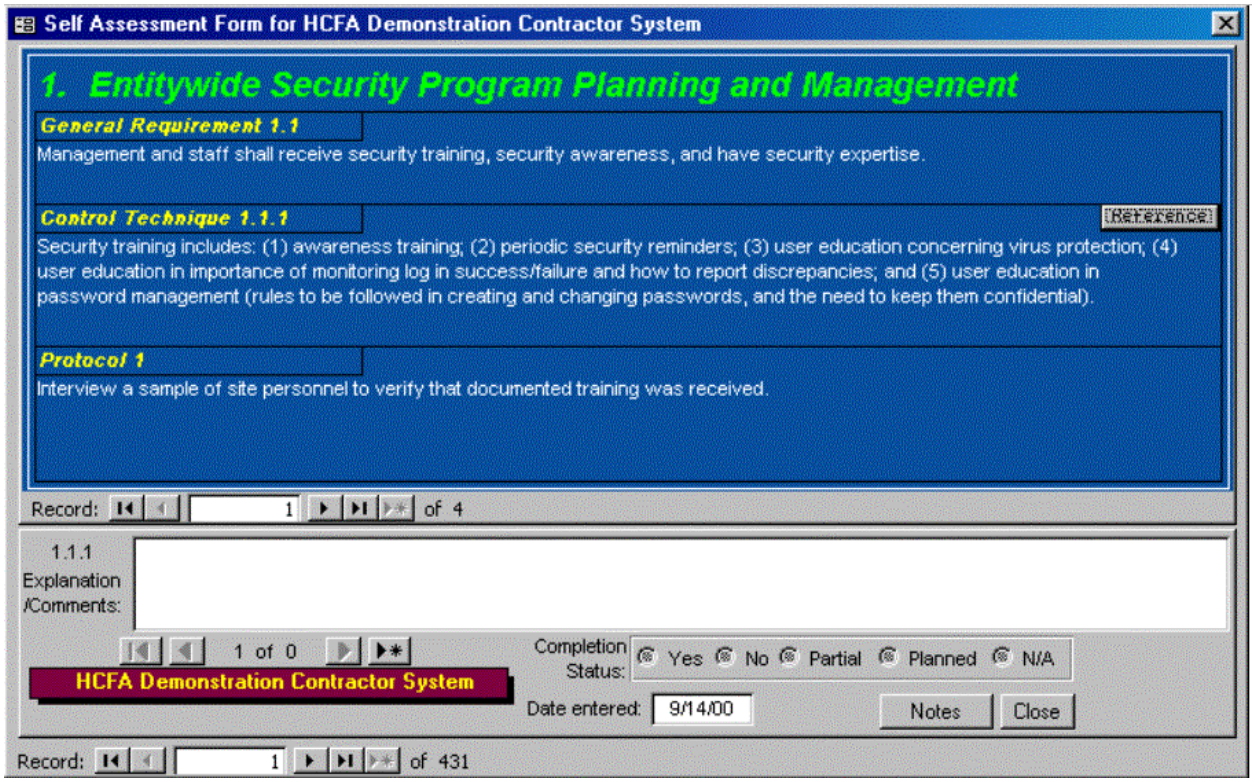

Figure A-2. CAST Self-assessment Form

Business partners are required to enter a comment or explanation for each self-assessment item of every status, as follows:

Yes - indicates that the systems or elements of operation conform to ***all*** aspects of the Control Technique. The Explanation/Comments field should contain:

- How exactly the Control Technique is met.
- What can be used to verify compliance.
- Where applicable documentation can be found.
- Who is the principle point-of-contact for questions involving this requirement.

Example Entry: *"Security Training is conducted during initial employees orientation and every year during the month of November for all employees and contractors. It includes all aspects outlined in the Control Technique as documented in company policy NG 7541-S3. The records of attendance are maintained by the corporate training office on the fifth floor of Bldg. #5 (cabinet #5). POC is Jim Socrates (401) 555-1212."*

No - indicates that the requirements of the Control Technique are not currently being met and there is no formal plan for meeting these requirements. The Explanation/Comments field should contain:

- Why this control technique is not being met.
- What is preventing corrective actions from being implemented.

- Where applicable documentation can be found.
- Who is the principle point-of-contact for questions involving this requirement.

Example Entry: *"Our file server system uses a Green Hat Linux 1.0 operating system. This version of Linux is hard-coded to display the password while entering. G. Iam Secure ((401) 555-1234) contacted (via phone) Green Hat (I. M. Programmer @ (651) 555-4321) on 8/31/00 to determine if an update to correct this discrepancy is underway. Mr. Programmer indicated that the password will continue to be displayed through the next revision but future changes are tentatively planned."*

Partial **-** indicates that the requirements of the Control Technique are not currently being met in their entirety. This can simply mean that one or more portions of a Control Technique are not being met. However, it is more likely that the requirements are being addressed and safeguards are implemented, but *not throughout the entire enterprise*. Enter a "Planned Completion Date" (required) and describe how the remainder of the system will be brought into compliance. Be clear and complete with these comments as this explanation with be part of the Corrective Action Plan as well as the Self-assessment submitted to HCFA. The Explanation/Comments field should contain:

- Why this Control Technique is not being met.
- What is being done to remedy the situation.
- Where applicable documentation can be found.
- Who is the principle point-of-contact for questions involving this requirement.

Example Entry: *"We use a mainframe and an offsite data storage facility connected via a T1 line and triple-DES encryption. However, the local corporate distributed network (WAN), which may house some administrative documents containing sensitive patient information, is connected via DSL and T1 lines to remote facilities without encryption. Network Encryption devices are currently on order. The POC in the security department is Iam Secure (401) 555-1234."*

Planned **-** indicates that the requirements of the Control Technique are not currently being met, but a plan of action exists to remedy the situation. Enter a "Planned Completion Date" (required) and describe how the system will be brought into compliance. The Explanation/Comments field should contain:

- Why this Control Technique is not being met.
- What is being done to remedy the situation.
- Where applicable documentation can be found.
- Who is the principle point-of-contact for questions involving this requirement.
- Enter a "Planned Completion Date" (required) and describe how the system will be brought into compliance.

Example Entry: *"A training plan and training materials do not exist for new employee orientation training. New employee training is being developed in a joint effort between the Security Department and the IT Training department. The security training outline is complete*

and on file in the corporate training office on the fifth floor of Bldg. #5 (cabinet #5). The training POC is Jim Socrates (401) 555-1212. The POC in the security department is Iam Secure (401) 555-1234."

N/A - The Explanation/Comments field for an N/A should contain:

- Why this Control Technique is not applicable.
- How you verified with HCFA.
- Where applicable documentation can be found.
- Who is the principle point-of-contact for questions involving this requirement.

Example Entry: *"This requirement describes required features of "security rooms". CSR 2.2.25 suggests "security rooms" as one several possible methods, but does not require one. We use "secured areas" and "appropriate containers" (CSR 2.2.19 and 2.2.5). This issue was discussed via letter to HCFA (12/15/98) and agreed to by the Regional Office (2/4/99). Both letters are on file in the security office located on the third floor of bldg. #3 (cabinet #3). POC is Iam Secure (401) 555-1234."*

CAST serves as the repository for the Corrective Action Plan (see Section 3.5 of the HCFA/Business Partners Systems Security Manual). When the Annual Self-assessment is conducted, those items recorded as "Partial," or "Planned" are considered to be the Corrective Action Plan. CAST entries for Partial or Planned items should include the following dates in the Explanation/Comments field:

- Date a particular safeguard can be procured or initiated
- Dates of various stages of implementation

The business partner will submit the CAST database to the CCMO for review (along with all other required security documentation, as described in Section 3 of the HCFA/Business Partners Systems Security Manual).

CAST is available for download on the HCFA web site.