CHAPTER 6, PART 2
IBM & IBM COMPATIBLE MAINFRAME SECURITY

1 BACKGROUND

The increased level of scrutiny at the regulatory and media levels has mandated that USDA protect the integrity, confidentiality and availability of its assets. IBM/IBM Compatible Mainframes process data for mission critical, departmental priority and sensitive systems in USDA and for IT service clients. Audits conducted in 2000 by the General Accounting Office (GAO), the USDA Office of Inspector General and independent contractors revealed that the implementation and administration of security on IBM mainframes does not meet the Federal Government's minimum security benchmarks for Automated Information Systems (AIS). The audits also revealed a large amount of USDA assigned high level system privileges and that these environments lacked standardized administrative and technical controls. Further, USDA's IBM and IBM Compatible Mainframe areas do not sufficiently assure that we can prevent or detect unauthorized use of our systems.

Currently, USDA employs three <u>different</u> security access control software <u>systems</u> in our IBM/IBM Compatible environments: Resource Access Control Facility (RACF) supplied by IBM, Top Secret Security (TSS) and Access Control Facility 2 (ACF2) supplied by Computer Associates. These security access control packages provide the following standard features in the IMB/IBM Compatible environments:

a The ability to restrict access to the computing environment to only preauthorized users or tasks;

b The ability to control access to data, applications, and system software to only authorized users and at specific levels (i.e., read, write, delete, modify);

c The ability to set general system-wide security parameters;

d The ability to set user, data, and application specific security parameters;

e The ability to audit any and all activities performed by the users and system;

f The ability to establish a centralized or decentralized security administration environment; and

g The ability to control input to and output from the system.

The purpose of the policy below is to establish and implement standardized security policy and procedures that apply without regard to the type of security access software utilized within the IBM and IBM Compatible Mainframe computing environments.

2 POLICY

a It is USDA policy that technical and administrative controls will be established and maintained on all Automated Information Systems (AIS) which process, store or transmit Sensitive but Unclassified (SBU) information to:

(1) Ensure individual accountability by uniquely identifying and authenticating each individual system user;

(2) Validate the users' access authorizations before allowing access to information or processes;

(3) Maintain an valid audit trail of user security related events; and

(4) Prevent unauthorized access to a user's residual data by ensuring all storage areas (disk, tape, etc.) are overwritten or data rendered inaccessible by a new program gaining that space. Storage areas being disposed of must be degaussed or physically destroyed before disposal.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with an updated timeline for completion. CS will monitor all approved exceptions.

3 SECURITY STANDARDS

a Mainframe and Server Security. The security systems on all UDSA AIS shall be configured to ensure that: no access is obtained unless explicitly granted; the least level of access is granted and maintained at all times; and access is granted to data, system and application programs only on a need-to-know basis.

The following standards provide the authorized minimum security standards for the USDA systems: IBM Resource Access Control Facility (RACF), Computer Associates (CA) Top Secret Security, CA-Access Control Facility (ACF2), MVS, VM, Customer Information

Control System (CICS), Time-Sharing Option (TSO), Database Management System (DBMS) and other technical manuals and appropriate project office developed applications documentation.

Each agency, that runs an IBM mainframe environment within the USDA domain, that processes, stores, and/or transmits USDA data, shall develop specific technical guidelines for appropriate implementation of their security system (RACF, CA-Top Secret, CA-ACF2). These guidelines shall be submitted to ACIO, Cyber Security for review and approval.

Agency guidelines must, at a minimum, state how the following information system protections are to be employed within all IBM/IBM Compatible environments:

b System Resources. The system owner will coordinate with the operating system programmer(s), operator(s), engineer(s), Information System Security Program Managers (ISSPM) and System Security Administrators to identify all system resources, components, datasets, and connections that are to be protected by the security system or other internal mechanism and their level of protections.

c Operating System. Only authorized system engineers or auditors shall have access permission to view critical operating system controls. Full auditing shall be activated at all times on these users. Each system engineer and operator must have a unique logon identification so that all actions can be clearly attributed to a given user.

No users will be profiled with access privileges at the operating system level using the default system user logon identification. The operating system level default logon shall be REVOKED or SUSPENDED and have all system-level accesses removed from it.

d Emergency Use (FIRECALL) Logon. Each organization shall establish a method for emergency access to the system and system resources by systems engineers, system operators, system administrators, and system security administrators. Note all references to User ID/ACID/User Logon/User Identification shall be referred to as Logon.

The purpose of the FIRECALL Logon(s) is to allow on-duty systems support personnel required access to the system and associated resources in the event of failure, either after-hours or when systems support personnel with the required access cannot be contacted in a timely manner. System access privileges assigned to the FIRECALL Logon(s) shall be at the minimum level required to allow trouble-shooting, disaster recovery, and return the system to operational status.

Access to the emergency use Logon(s) shall be kept strictly on a need to know basis. Each site shall establish policy and procedures for controlling access to this logon and auditing its use. Each use of the emergency use Logon(s) shall be audited by the system. The computer operations manager who accessed it shall notify the system security administrator in writing immediately the next workday of the use of the emergency use Logon(s). The memo shall include the reasons for use and who used it. The system security administrator shall immediately change the password (which may be set to never expire) on the emergency use Logon(s) and reseal it in an envelope and return it to the locked storage cabinet. On a daily basis, the security administrator will run an audit report on the Emergency Use Logon(s to verify their status and use history.

e Logon Guidelines. Individual accountability shall be enforced by the system by uniquely identifying each user to the system (i.e., each Logon may be assigned to only one authorized user). Under no circumstances shall multiple users ever share a Logon.

f Logon Revocation Due to Non-use. Policy and procedures shall be established for each IBM/IBM compatible mainframe system that specify at what interval and how user Logon IDs shall be rendered inactive/suspended/revoked due to non-use. (Both RACF and Top Secret System can be configured to automatically suspend user accounts after specified periods of non-use). The action taken by the system or security administrator shall make it impossible for these user Logon IDs to access the system, data, or resources without overt action by the security administrator to reinstate Logon privileges. The maximum interval for non-use of a user Logon ID prior to deactivation shall be 30 days for general users and 15 days for privileged users. Users who require a longer interval of non-use prior to revocation should be handled individually or placed in separate groups for administrative purposes; written justification should be kept on file by the security administrator for the longer interval.

g Passwords. All passwords shall be at least 6-8 characters in length and alpha-numeric in composition (this shall be enforced systemically by the security or operating system). The password files must be encrypted. Passwords shall not be transmitted in clear text.

Maximum lifetime for a password is 60 days for general users; and 30 days for privileged users (e.g., Security Administrators, programmers, auditors, engineers). Password history for each user shall be maintained systemically. The setting shall not be less than 5. Users' logon shall be automatically revoked by the system after three (3) consecutive unsuccessful password attempts. As a routine courtesy, the users may be notified by the system in advance that their password will expire. System passwords, such as for started tasks and batch jobs can be set to never expire, however, access to these resources must be protected and audited by the security system.

Logons and passwords shall not be automated through use of functions keys, scripts, or other methods where logons and passwords may be stored on systems. Exceptions are pass-through communications and system calls. All vendor supplied (default) passwords, including those for software packages and maintenance accounts, are to be changed as soon as a system or product has been installed.

h Discretionary Access Controls (DAC). The system shall define and control access between named users and system components (e.g., files, datasets, and programs). The system or network users may be provided the capability to specify who (by individual user or users, group, etc.) may have access to their data. The system or network shall be configured to ensure that users without specific authorization are not allowed access to data or resources.

Discretionary Access Controls are used to implement security policy that ensures that no one can access our computers without being authorized. No one will be permitted access to computer data without being explicitly authorized. No one will access resources (i.e., data, programs, libraries, remote connections, etc.) without being duly authorized. No one can change the access rules or profiles without being explicitly authorized. There will be adequate separation of authority and duty for computer system and security administration. No process or function can be initiated on the system without verification of authorization. Security software controls will be implemented and maintained on USDA systems to provide access only if explicitly granted and at the least level of access that is necessary for the function. Software controls will assure that access is granted to data and resources only on a need-to-know basis. No System Started Procedures, Tasks, Batch Jobs, or Programs will be allowed to bypass the security checks or change the 'Problem Program State' of an application or program to the Supervisor State unless specifically authorized in writing by the Accrediting Authority.

All information system security environments will be carefully established and periodically verified to ensure need-to-know access is maintained. Each agency will conduct an annual review of user access privileges to verify continuing access requirements. A systematic analysis of access configuration should be performed whether setting up the security system for the first time or conducting a top-to-bottom review and verification of access controls. A review team should be designated that includes systems personnel as well as individuals from the business function. This group could include but is not limited to the application manager or owner, system programmers, system administrators, security administrators and database administrators, business function manager. All access points and resources that are connected to the system should be identified (e.g. CPUs, applications, remote ports, remote job entry sites, TSO, CICS, DASDVOL, databases, batch jobs, started tasks, etc.). Each of the access points and resources requires a call to the security software so that only specifically defined users and resources can use the system. All users with TSO logon are required to be defined to the security system. All started tasks shall have a User ID or Access Identification (ACID) associated with them and must be identified to the security system. Business owners should determine who must have access to resources to perform their jobs (e.g., programmers, system administrators, security administrators, database administrators, end-users).

Access profiles for users and resources should be developed based on similar access requirements (e.g., test system, production code maintenance, application access only, etc.) Access privileges should be specified based on: no access unless explicitly granted, need-to-know, and least level of privilege. The Delegation of Authority for the administration (centralized vs. decentralized) should be determined for the system including the security function. The power a user needs while connected to a specific functional group, whether it be group level controls for administration or only read access to specific datasets should be determined. Business owners should determine dataset and resource access rules and profiles (universal access and permission lists). The agency administering the operating system should ensure that System Started Tasks, Procedures, and Programs are prevented from bypassing security checks and auditing, unless specifically authorized by the DAA.

i Minimum Systemic Controls. All logon/logoff activity, program calls, uses of system privileges, security command violations will be logged by the system. All security related actions/commands will also be logged. All resources classes activated on a given IBM system will be identified to the security system and all failed access attempts and changes to the resource shall be logged. Controls will be established and maintained to ensure that all batch jobs executed on the system are associated with a valid User ID or ACID. All datasets must be defined to the security system to ensure that only authorized users can gain access. Internal policy and procedures must be established by each agency to ensure that unauthorized access to a user's residual data cannot be obtained. Within production parameters the security system's OBJECT REUSE function should be activated. If this function cannot be implemented without undue impact on system processing overhead, then the agency must document and implement mechanisms it has in place to ensure that residual data and applications cannot be compromised. If the security system's OBJECT REUSE function is not activated then a exception must be obtained from the OCIO. Datasets stored on current RAID DASD technology do not require the OBJECT REUSE function as deleted datasets are not recoverable. Datasets stored on tape must be protected from unauthorized access by using a security management system or tape management system or both. All data storage devices shall be rendered unreadable by degaussing, overwriting (5-7 times with random 1's and 0's) or complete physical destruction prior to disposal.

Access by inactive users should be suspended by the system after 30 days (maximum). Password syntax must indicate 6-8 characters, alpha-numeric (shall be enforced by the security system). All system default passwords must be redefined by the installation. All remote accesses to the system must be defined to the security system. All accesses to APF libraries shall be specifically defined (no universal access). All installation defined program exits must be reviewed by the Office of Cyber Security and approved in writing by the agency DAA.

j Minimum System Resources to be Protected. The following list of system resources must be secured:

(1) Started Tasks (must be audited)
(2) APF Libraries (must be defined to the security system and access strictly limited to need-to-know)
(3) SYS1.UADS
(4) SYS1.PARMLIB
(5) SYS1.VTAMLIST
(6) SYS1.PROCLIB
(7) SMF data
(8) Security system exits
(9) JES2 Spool display software
(10) All TSO authorized accesses (must be strictly controlled and audited for unauthorized access)
(11) All BATCH Jobs (must be subjected to security checks for submission by authorized users)
(12) No programs shall be allowed to bypass security checks without the written authorization of the DAA
(13) All SVCs (whether user defined or site-modified vendor–supplied shall be documented)
(14) All operating system, application, resource, and security exits must be documented and approved by the DAA
(15) LINKLIST libraries

(16) System Catalogs
(17) SYS1.NUCLEUS
(18) System-level product installation libraries
(19) JES SPOOL dataset
(20) SYS1.DUMP
(21) System backup files
(22) SYS1.TRACE
(23) System commands
(24) System console devices (e.g. password controlled screen lock, physical controls)

k Review of Audit Reports. The SSA will review Security (Command Violations) Reports daily. Suspicious activity shall be referred to the agency IT manager and ISSPM for review and disposition.

3 RESPONSIBILITIES

GENERAL

Each USDA site operating an IBM mainframe system shall assign a Security System Administrator (SSA), and backup security system administrators as necessary for that system. The SSA has overall responsibility for administration and maintenance of the implementation of the user and group access profiles for systems under his or her jurisdiction.

Maintenance and modifications to these environments (system or application), other than user profiles, are to be directed and controlled by a formal configuration management/change transmittal system.

Security administration is an independent responsibility and shall not be assigned to a System/Application Programmer, Database Administrator, System Administrator, or System Operator. Security personnel must, however, work closely with all system administration personnel to maximize system performance and security.

a The Associate CIO, Cyber Security will:

(1) Conduct periodic security assessments on IBM/IBM Compatible mainframe computing systems;
(2) Review mainframe computer system security guidelines and standards;
(3) Review mainframe computer system security plans;
(4) Review and coordinate requests for deviations and exceptions pertaining to mainframe computer systems with the Associate CIO for IRM; make recommendations regarding exceptions to CIO and
(5) Review mainframe computer system Certification and Accreditation documentation.

b The Agency Chief Information Officer will:

(1) Ensure that sufficient resources are applied to the IT security function to ensure that mainframes and servers have mandated protection;
(2) Ensure all personnel acknowledge in writing the system security requirements and their responsibilities pertaining to security;
(3) Ensure that separation of duties among IT staff is maintained to avoid a conflict of interest;
(4) Ensure a list of SBU systems and applications (operational and under development) at the site is maintained, providing the name and a brief description;
(5) Ensure that certification and accreditation activities and documentation (i.e., risk assessment, security plan, disaster recovery plan, privacy impact assessment, trusted facility's manual, etc.) are complete and maintained;
(6) Ensure that the most current copy of the signed certification and accreditation report for each system and application is on file;
(7) Ensure a file copy of all approved exceptions to an information system's security requirements is maintained and available;

(8) Ensure that security tests and evaluations are performed for each agency information system being developed or maintained;

(9) Ensure software is in compliance with copyright agreement and software license;

(10) Review audit reports of accounting, adjustments, and other Critical financial functions and coordinate review of any suspicious activities with the CS program;

(11) Ensure that audit trails are appropriately reviewed; IT managers will notify the SSA within 3 working days of action taken on suspected security violations;

(12) Ensure that functional security reviews are conducted;

(13) Assure that any moves or changes to an information system are coordinated with the system security function;

(14) Maintain documentation that details the information systems hardware and software configurations at each facility;

(15) Ensure that appropriate technical, administrative, physical, and personnel security requirements in the specifications for acquisition or operations of information systems are documented, reviewed and approved by the management official responsible for security at the facility operating the information system;

(16) Ensure security requirements (which include personnel and physical security) are incorporated in the planning phase and continued during each phase of the life cycle;

(17) Ensure that the system development project plan includes: when and how the security requirements will be identified; security safeguard development efforts during the project design phase; security test criteria during the testing phase and accreditation and certification effort during the acceptance phase;

(18) Ensure that security requirements, features, and techniques are:

(a) Incorporated during the planning and conceptual phase for all new systems, applications and telecommunications systems that store, process, transfer, or communicate sensitive but unclassified (SBU) information;

(b) Defined and approved prior to acquiring or starting formal development of all information systems and applications and reviewed throughout the life cycle;

(c) Kept current throughout the entire life cycle of the system or application;

(d) Precise enough to allow tests to be designed that will determine if security requirements are satisfied;

(e) Reviewed by all organizations involved in the use and operation of the information system or application; and

(f) Included as part of the management control process for SSI information systems and applications.

(19) Ensure that system design reviews are:

(a) Conducted to ensure that the proposed design meets the security specifications and the review findings are approved prior to detailed design and programming;

(b) Initiated prior to placing an information system or application into operation to ensure that the proposed system complies with approved security specifications;

(c) Included as part of the management control process for SSI information systems and applications; and

(d) Documented and records of the results maintained.

(20) Ensure testing of security features is:

(a) Conducted by a third party who acts independently of the development organization, in addition to development testing;

(b) Performed periodically to assure that security features work as claimed in the system's documentation;

(c) Conducted to ensure that there are no obvious ways for an unauthorized user to bypass or defeat security features of the information system or network;

(d) Conducted to ensure that the proposed information system or application meets the approved security specifications prior to placing the information system or application into operation;

(e) Performed after installation of an information system or product;

(f) Included as part of the management control process for SSI system and information; and

(g) Documented and the results maintained.

(21) Ensure that all system software development, experimentation, testing and debugging is performed in an information system dedicated for these purposes and does not contain or use “live” data; and

(22) Ensure that tests are performed to evaluate the security related code;

(23) Grant users access to sensitive but unclassified data on a need-to-know basis and cancel access when no longer needed;

(24) Assign and periodically review user access permissions so that capabilities such as authorizing, recording, issuing, and receiving are assigned to different individuals to minimize the possibility of fraud, waste and abuse;

(25) Periodically review users’ access profiles for required changes;

(26) Annually certify that profiles and accesses for each employee have been reviewed and are appropriate; and

(27) Ensure audit trails and reports are reviewed regularly for irregular activity.

c The agency Information System Security Program Manager/Designate will:

(1) Ensure that security orientations are given to users prior to their use of an information system;

(2) Ensure users acknowledge, in writing, that they understand the information system security rules;

(3) Notify user's management, Cyber Security and the System Administrator of any unusual user activity or security violations;

(4) Annually conduct a complete review of users' access privileges to verify continuing access requirements;

(5) Maintain a copy of the user access request form for each user accessing the information system;

(6) Ensure all information system users and USDA contractors have prior approval and the appropriate level of background investigation at least initiated before granting them access to information systems;

(7) Ensure that management verifies information system user's employment with Personnel/Human Resources prior to granting access to computer systems and data;

(8) Ensure all personnel who install, operate, maintain, or use an information system have authorized access and are familiar with documented security practices before granting them access;

(9) Coordinate and implement a security training and awareness program;

(10) Selectively audit actions of one or more users based on an individual's identity;

(11) Inspect and monitor user files only with the Designated Accrediting Authority (DAA) approval;

(12) Periodically monitor a system's use by reviewing audit trails;

(13) Develop and coordinate audit procedures with other internal control procedures required under OMB Circular No. A-123, Management Accountability and Control;

(14) Review the use of audit trails and audit reports;

(15) Use audit trail capabilities to ensure system integrity and examine a system's audit log regularly and report abnormalities to the Agency IT Manager;

(16) Perform technical reviews of security certification documentation (e.g., Security Plans, Risk Assessments, Disaster Recovery Plans) to ensure they are sufficient and complete;

(17) Conduct annual security compliance reviews as well as random security checks for each information system under their authority to ensure security procedures and requirements are in compliance with agency directives;

(18) Review system and related software security vulnerabilities and ensure that appropriate countermeasures and patches are applied;

(19) Evaluate the effectiveness and impact of security measures and features and report any existing or potential problem areas to the appropriate DAA;

(20) Distribute necessary directives that implement Departmental information system security policies to be used at remote facilities and terminal areas, and monitor their implementation;

(21) Prepare and submit a written report to the appropriate DAA of all technical security exceptions, outline the risks and vulnerabilities that could result from granting exceptions and identify other alternatives;

(22) Coordinate or participate (as required by the Agency IT Manager) in the preparation of disaster recovery and business resumption plans for each essential or critical information system; and

(23) Periodically reviews the approved Configuration Management (CM) documentation that details the information systems hardware and software in the Program Library for all agency information systems to ensure that systems and applications are accredited and documentation is complete.

d Agency System Security Administrators/Designates (responsible for administration of security software) will:

(1) Assign the initial user identifications and passwords with organization security coordinator;

(2) Add, delete, or modify user access in coordination with user organization security coordinators and agency IT Management;

(3) Maintain a master list of system users;

(4) Verify and maintain a current hardware, application, and software inventory for systems under their authority;

(5) Ensure access to software systems is strictly controlled;

(6) Review system and related security vulnerabilities; the SSA will review the Security (command violations) Report for all AIS on a daily basis; all suspicious activity will be flagged, researched and referred to the IT Manager and agency ISSSPM for review;

(7) Evaluate the effectiveness and impact of system or application security measures and report any existing or potential problem areas to the appropriate DAA through the agency ISSPM;

(8) Ensure that the ISSPM is informed of any major changes to systems hardware or software;

(9) Initiate proactive or corrective countermeasures if a security problem develops in accordance with DM3500-1, USDA Computer Incident Response Procedures Manual;

(10) Promote security awareness with system and application users;

(11) Coordinate customer engineer access for design applications and system changes;

(12) Generate audit trails and distribute to the appropriate agency IT Managers and user organization security coordinator;

(13) Ensure that all personnel who install, operate, maintain, or use an information system have authorized access and are familiar with documented security practices before granting system access; and

(14) Ensure that system's software packages are properly stored and protected.

-END-