CHAPTER 8 – PART 2
Risk Assessment and Security Checklists

1 BACKGROUND

The United States Department of Agriculture houses and processes sensitive data, including personal information of US citizens, payroll and financial transactions, proprietary information and life/mission critical data. It is essential that this information be protected from the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction.

To assist USDA agencies in identifying potentially harmful deficiencies in their respective security programs and security controls, a set of security checklists have been developed. This set includes checklists for the following platforms, environments and operating systems:

General Checklist for Security Programs
Microsoft Windows NT For Servers
Microsoft Windows NT For Workstations
Microsoft Windows 2000 for Servers
Microsoft Windows 2000 for Workstations
UNIX for Servers
UNIX for Workstations
Telecommunications
Personal Electronic Devices
IBM AS/400 Systems
Software Development Environments
Mainframe Environments
Web Farm Environments
Classified Systems

2 POLICY

Each USDA agency and staff office shall conduct an assessment of it's security program every year, using the USDA General Security Checklist. The assessment shall be completed during

the fourth quarter of the fiscal year. Results of the assessment shall be submitted to OCIO's Cyber Security Program.

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 a updated timeline for completion. CS will monitor all approved exceptions.

3 PROCEDURES

a Review of Security Controls. Assessments of all GSS and MA, whether USDA owned and operated or contractor owned and operated are required whenever a major change is made to the system, or at least every three years. Assessments could include applications such as databases and spreadsheets depending on the sensitivity of the data, inherent risks, mitigation costs and value of assets. Each agency is responsible for making this determination. These assessments shall be completed using one or more of the security checklists developed for USDA. The number of checklists to be used will depend on the operating systems and the technical environments that comprise the system. For example, a single system may require the execution of a UNIX checklist, a Mainframe checklist and a Telecommunications checklist in order to ensure that all necessary security controls are considered.

Checklists may also be used by agencies for any GSS system, such as operational environments and their program products where deemed necessary to protect the confidentiality, integrity and availability of information

and the application or data they support. The checklist will be used at the GSS level and augmented by a review of the application access controls.

Results of these assessments will be submitted to OCIO's Cyber Security Program 30 working days after completion of the assessment. Both the checklists and the results are considered highly sensitive and to be released to USDA employees or contractors only on a "Need to Know" basis. We strongly urge that a Non-Disclosure Agreement be signed prior to release.

b System Development Assessment. For every system that is developed or managed under contract, the requirement for an assessment using the appropriate checklist(s) will be incorporated into the contract security requirements. A risk assessment will be performed in conjunction with system development. At a minimum, this assessment will include the execution of one or more security checklists developed for USDA. The number of checklists to be used will depend on the operating systems and technical environments that comprise the system.

Results of these assessments shall be included with other documentation submitted to OCIO for exception requests or in conformance with the Capital Planning and Investment Control (CPIC) requirements.

c Checklist Revision and Version Control. Agencies are encouraged to request changes to security checklist at any time to ensure they are current and relevant. At least once annually, OCIO will hold a checklist update session for each checklist to ensure completeness and that all question remain germane. Prior to executing any checklist for any purpose, agencies shall contact OCIO/Cyber Security to obtain the most recent version.

4 RESPONSIBILITIES

a The Chief Information Officer/Deputy will:

(1) Support the USDA Risk Management Program for the protection of USDA Information Technology assets; and

(2) Encourage agencies to perform assessments using Security Checklists.

b The Associate CIO for Cyber Security will:

(1) Develop and maintain policies, tools, and techniques for assessing risk to USDA information systems;

(2) Provide training and guidance to agencies for identifying risks and vulnerabilities to the information systems they use and maintain;

(3) Review the results of assessments conducted by agencies;

(4) Assist agencies in devising appropriate risk mitigation strategies, as required; and

(5) Review all exception requests and capital planning documentation to ensure risks have been assessed prior to deployment of all USDA General Support Systems and Major Applications.

c The Associate CIO for Information Resources Management (IRM) will:

(1) Support the policy and procedures contained in this chapter to ensure that the USDA Risk Management Program is used in all USDA managed networks, systems and servers; and

(2) Receive, review and coordinate a response with the Associate CIO for Cyber Security to any exception requests for exceptions to this policy.

d The Agency Chief Information Officers will:

(1) Ensure that information system security controls are selected and implemented commensurate with identified risks;

(2) Ensure that all agency personnel, especially the Agency Information System Security Program Manager (ISSPM), are aware of the policy and procedures concerning assessments;

(3) Ensure that assessments are conducted as prescribed in this policy by IT personnel or anyone delivering services via an IT system; and

(4) Report the findings of assessments promptly to OCIO/Cyber Security as defined in the procedures section;

(5) Ensure that all completed Checklists are kept in a secure location and that access is granted on a need to know basis; and

(6) Provide access to assessment results which are considered to be sensitive on a need to know basis.

e The agency Information System Security Program Managers/staff will:

(1) Conduct or coordinate assessments as prescribed in this policy;

(2) Ensure that checklists and results are protected and released on a need to know basis;

(3) Coordinate checklist change requests for their respective agency and submit to OCIO/Cyber Security; and

(4) Participate in the checklist development, training and maintenance process.

-END-