Mission Area Directive	MRP 3140.5	10/31/2019

MRP INFORMATION SYSTEMS SECURITY (ISS) ROLES AND RESPONSIBILITIES

TABLE OF CONTENTS

1. PURPOSE

This Directive establishes the policy and roles and responsibilities to support the Information Systems Security Program (ISSP) for the Marketing and Regulatory Programs (MRP) Mission Area and its agencies, Animal and Plant Health Inspection Service (APHIS) and Agricultural Marketing Service (AMS).

2. SPECIAL INSTRUCTIONS AND REPLACEMENT HIGHLIGHTS

a. This Directive supersedes APHIS 3140.5 APHIS Information Systems Security (ISS) Roles and Responsibilities, dated 8/23/2013.

b. This Directive is in force until cancelled or superseded.

3. AUTHORITIES AND REFERENCES

This Directive must be applied in conjunction with:

a. American Disabilities Act (ADA) of 1990 (Section 508 Compliance).

b. Computer Security Act of 1987.

c. Clinger-Cohen Act.

d. E-Government Act of 2002.

e. Computer Fraud and Abuse Act.

f. Presidential and Federal Records Act.

g. Paperwork Reduction Act of 1995.

h. Privacy Act of 1974.

i. USDA Departmental Manual (DM) 3515-000 Privacy Requirements.

j. USDA DM 3515-002 Privacy Impact Assessment.

k. USDA DM 3550-002 Sensitive but Unclassified Information Protection.

l. USDA Department Regulation (DR) 3080-001 USDA Records Management Regulations.

m. USDA DR 3545-001 Information Security Awareness and Training Policy.

n. USDA DR 3540-003, Security Assessment and Authorization.

o. USDA DR 3545-001 Information Security Awareness and Training Policy.

p. MRP Directive 3020.1 Forms Management Program.

q. MRP 3140 Information Systems Security Handbook.

r. Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources.

s. National Institute of Standards and Technology (NIST) Special Publication 800-61, Computer Security Incident Handling Guide.

t. NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, Test Procedures.

u. USDA MRP Strategic Plan 2018-2022.

v. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

4. ACRONYMS/ABBREVIATIONS

a. A&A – Assessment and Authorization

b. ACIO – Assistant Chief Information Officer

c. AO – Authorizing Official

d. AMS – Agriculture Marketing Service

e. APHIS – Animal and Plant Health Inspection Service

f. ATO – Authorization to Operate

g. BIA – Business Impact Analysis

h. CAB – Change Advisory Board

i. CDM – Continuous Diagnostic and Mitigation

j. CISO – Chief Information Security Officer

k. CSAM – Cyber Security Assessment Management

l. CSSD – Cyber Security Services Division

m. DATO – Denial of Authorization to Operate (DATO)

n. FISMA – Federal Information Security Management Act

o. IMB – Information Management Branch

p. ISA – Interconnection Security Agreement

q. ISSM – Information System Security Manager

r. ISSO – Information System Security Officer

s. ISSP – Information System Security Program

t. ISSPM – Information System Security Program Manager

u. MOA – Memorandum of Agreement

v. MOU – Memorandum of Understanding

w. MRP – Marketing and Regulatory Programs

x. NIST – National Institute of Standards and Technology

y. PIA – Privacy Impact Assessment

z. POA&M – Plan of Action and Milestone

aa. PTA – Privacy Threshold Analysis

bb. RBD – Risk Based Decision

cc. RMF – Risk Management Framework

dd. ROB – Rules of Behavior

ee. SDLC – System Development Lifecycle

ff. SOO – Statement of Objectives

gg. SOP – Standard Operating Procedures

hh. SOW – Statement of Work

5. SCOPE

a. This Directive applies to all MRP employees who use MRP information systems to accomplish MRP business functions. All of the aforementioned are considered users and are included wherever the words “user” or “users” are referenced within this Directive. Non-MRP users must comply with the training.

b. MRP information systems covered by this Directive include all information systems that process, store, or transmit data in support of the MRP mission area. This includes all computer hardware, software, telecommunications equipment, mobile devices, or other information resources that comprise the MRP network of general support systems or applications and services they support.

6. POLICY

a. MRP CISO must ensure that the responsibilities outlined in this Directive for each role are implemented within the Program.

b. All MRP users will participate in the ISSP and must perform their duties in ways that support ISSP functions.

c. In keeping with the philosophy of "least privilege", users will be provided access to and use of only those information resources needed and systems will be installed, operated, and maintained with only those features or services required to satisfy official business requirements in support of the MRP Mission Area.

d. MRP has a specific responsibility to protect information resources and will comply with all Federal and Departmental policies, regulations, and requirements.

e. All employees who work with MRP resources are individually and personally responsible for applying the appropriate security measures and for complying with Federal, USDA, and MRP policies and procedures on the subject. Willful failure to comply may result in punishment, including dismissal, under the Computer Fraud and Abuse Act and other appropriate Federal statutes.

f. Exceptions to the requirements of this Directive are only authorized if approved in writing by the MRP Assistant CIO.

7. ROLES AND RESPONSIBILITIES

a. The APHIS and AMS Administrator will ensure that MRP has an established ISSP that:

(1) Provides information security protections commensurate with the risk in consideration of the magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.

(2) Ensures that information security management processes are integrated with Agency strategic and operational planning processes.

(3) Delegates to the ACIO for MRP the authority to ensure compliance with the requirements imposed by FISMA.

NOTE: The MRP ISS is the responsibility of APHIS since MRP-IT resides under APHIS.

b. APHIS Designated Program Deputy Administrators/AMS Associate Administrator or their designee must serve as the Authorizing Official (AO) for systems in their programs. The AO is a USDA program executive with the authority to evaluate the mission, business case, and budgetary needs for the system in view of the security risks present in the system's operating environment.

NOTE: MRP uses the AO title instead of Designated Authorizing Agent (DAA) to be compliant with NIST and Federal requirements.

c. The Authorizing Official (AO) will:

(1) Appoint a Business System Manager to work collaboratively with the System Owner, Information System Security Manager (ISSM) and Information System Security Officer (ISSO) to ensure that IT systems are compliant with security and privacy requirements.

(2) Appoint a system owner to a FISMA reportable system, developmental system, or a cloud-based platform.

(3) Ensure that the system is being assessed and authorized within the approved MRP-IT fiscal year workload leveling plan which is determined by the System Owner and ISSM.

(4) Assume responsibility for the residual risks of operation of the system.

(5) Formally approve the operation of an IT system at an acceptable level of risk within its environment by issuing an authorization decision. Note it is recommended that the Authorizing Official designate an Acting Official to sign off on Authorization to Operate (ATO) memo while he/she is not available. Authorization decisions include the issuance of:

(a) Authorization to Operate (ATO). If, after assessing the results of the security certification and the Concurrency Review memoranda, the AO deems that the risk to Agency operations, Agency assets, or individuals is acceptable, and the criteria of the concurrency review memoranda will be met, an ATO is issued for the information system. If the requirements of the memoranda cannot be met, then a request for an extension will be submitted.

(b) Denial of Authorization to Operate (DATO). If, after assessing the results of the security certification, the AO deems that the risk to Agency operations, Agency assets, or individuals is unacceptable, the authorization to operate the information system will be denied.

(c) Previous Authorization. In the event that a new AO is assigned responsibility for the information system, the newly assigned AO will review the current security authorization package (i.e., authorization decision, decision rationale, and terms and conditions) and the current system status reports to determine if a reauthorization action is warranted. If the new AO is willing to accept the known documented risk, then reauthorization occurs only when there is a significant change to the information system or when a specified time period has elapsed in accordance with Federal or Agency policies.

(d) Approved security requirements documents to include: Memoranda of Agreement (MOA), Memoranda of Understanding (MOU), Interconnection Security Agreements (ISA), and any risk based decisions.

(e) Ensure that the annual mandatory Security Awareness and Rules of Behavior training is completed by employees, contractors, affiliates, and students.

(f) Ensure that the assigned annual mandatory Specialized Training is completed by employees, contractor, affiliates, and students.

d. The Assistant CIO for MRP (MRP ACIO) will:

(1) Approve and issue MRP ISSP policies and guidance that establish a framework for an ISSP to be implemented by MRP.

(2) Monitor, evaluate, and report to the Administrators on the status of information systems security within MRP.

(3) Designate, in writing, a Chief Information Security Officer (CISO) to execute the MRP ISSP.

(4) Serve as the certification agent for all FISMA reportable information systems and will:

(a) Certify the results of Assessment and Authorization (A&A) security assessments which include the management and technical security controls of information systems.

(b) Determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome in meeting the security requirements for information systems.

(c) Provide the recommended corrective actions to reduce or eliminate vulnerabilities in information systems.

(d) Provide independent assessments of the system security plan to ensure the plan adequately describes the security controls for the information system. The certification agent must be in a position that is independent of individuals who are responsible for:

1. Development of the information system.

2. Day-to-day operation of the information system.

3. Correction of security deficiencies identified during the security certification.

NOTE: The independence of the certification agent is an important factor lending credibility to the security assessment results and

ensuring the AO receives the most objective information possible in order to make an informed, risk-based, authorization decision.

e. The MRP CISO will:

(1) Serve as the primary liaison to the Assistant CIO for MRP, Authorizing Officials, USDA CISO, and other USDA Agency CISOs.

(2) Appoint an Information System Security Program Manager (ISSPM). Note that there is an ISSPM for both the Operations and Risk and Compliance branches.

(3) Appoint in writing, an Information System Security Manager (ISSM), Information System Security Officer (ISSO) or Project Manager (PM), and alternates, to implement the MRP ISSP requirements. Assignment letters must be maintained on file for the duration of the employees' appointments.

(4) Develop, document, and implement an Agency wide ISSP.

(5) Develop and update as required, ISS policies, procedures, and control techniques.

(6) Assist Agency officials in carrying out their FISMA responsibilities.

(7) Ensure information systems security is included in initiatives such as new project intake, strategic planning, and enterprise architecture.

(8) Monitor and evaluate the status of information systems security in MRP by performing annual compliance reviews of program and system controls.

f. The MRP ISSPMs will:

(1) Provide information system security guidance and technical assistance to all program units.

(2) Monitor MRP level weaknesses and monitor program level weaknesses reported as a result of self-assessments and external reviews using the FISMA security management tool.

(3) Identify resource requirements, including the funding and personnel needed to efficiently manage the MRP ISSP.

(4) Lead MRP certification teams in support of the Assistant CIO for MRP certification duties.

g. The Security Operations will:

(1) Coordinate to ensure timely patching and non-patch remediation of MRP systems and products to correct security problems in software and firmware. This specifically relates to chairing the MRP Patch and Vulnerability Working Group (PVWG), coordinating with MRP-IT Services Infrastructure Services Division to engineer remediation fixes for vulnerabilities for which no patches exist, and reporting patch and vulnerability status to management and Programs.

(2) Ensure MRP Incident Response Plan and Standard Operating Procedures (SOPs) are updated regularly at least once a year, and provide oversight to the MRP Computer Incident Response Team (MCIRT) to ensure that MRP security and PII incidents are handled in a timely manner in accordance with the MRP Incident Response Plan and SOP.

(3) Serve as the main overall point of contact for coordinating the planning and implementation of the USDA Continuous Diagnostics and Mitigation (CDM) program initiative in MRP.

(4) Conduct monthly and ad hoc vulnerability scanning and generate reports for remediation.

(5) Participate in MRP CAB change management meetings.

(6) Monitor security appliances to include and manage vulnerability appliances.

(7) Test the incident response capability using tests and conduct Contingency and Disaster Recovery exercises annually as defined by the system owner to determine the incident response effectiveness.

h. The MRP-IT Infrastructure Services Division will:

(1) Be responsible for the patching as below:

(a) Participate in the PVWG meetings.

(b) Submit Requests for Change (RFC) to the MRP Configuration Advisory Board to start the change management process.

(c) Schedule test deployments and resolve testing issues to ensure applications do not break.

(d) Communicate patch deployments to MRP employees as needed.

(e) Schedule patch deployment.

(2) Provide support to MCIRT for handling and resolving security and PII incidents in accordance with the MRP Incident Response Plan and SOP.

(3) Assist CSSD with the remediation of vulnerabilities related to the MRP Enterprise Infrastructure General Support Systems – APHIS Enterprise Infrastructure (AEI GSS) and AMS Infrastructure WAN and DMZ (AMSWAN), cloud systems, and infrastructures by:

(a) Reviewing the vulnerabilities and identifying those responsible for remediating.

(b) Remediate the vulnerabilities by the scheduled completion date.

(c) Document risk-based decisions (RBD) by using the USDA template for low risk vulnerabilities as determined by management and CSSD.

(d) Regularly update Plan of Action and Milestones (POAMs).

(e) Provide remediation updates and reports to management and CSSD as requested.

(f) Assign project managers for the AEI GSS and MRP-IT managed cloud systems and services to ensure compliance with the information security requirements specifically the A&A in accordance with MRP, USDA, and Federal requirements.

(4) Include CSSD to participation in new technology assessments, design, and implementation.

i. The Strategic and Customer Services Division will:

(1) Participate in the MRP-IT planning and implementation process to ensure that all MRP-IT system security requirements are implemented and maintained within program units according to the Paperwork Reduction Act, Federal Records Act, and E-Government Act.

(2) Assist CSSD with the creation and remediation of POAMs that the Information Management Branch (IMB) assist in remediating.

(3) Notify CSSD of any new systems or investments pertaining to the MRP-IT Portfolio. Including sharing new investment/new system

documentation that Portfolio and Budget Management Branch (PBMB) receives from the programs.

j. The Program Business System Manager will:

(1) Work collaboratively with the system owner to define business requirements for the IT system.

(2) Work with the system owner in determining the Security Categorization of a system.

(3) Assist the system owner with the Privacy Threshold Analysis (PTA) and, if need be, the Privacy Impact Assessment (PIA).

(4) If needed, be responsible for development of the System of Record Notice (SORN).

(5) Complete a Business Impact Analysis (BIA) for the assigned information system.

(6) Complete Records Scheduling Request (MRP Form 400) and submit to IMB.

(7) Notify the CISO, ISSM, and IMB of any proposed IT systems.

k. System Owners, as identified within their Agency/Program, are responsible for the day-to-day management and operations of applications and systems under their purview. In accordance with USDA DM 3555-01, A&A, system owners will:

(1) Ensure A&A is maintained for all current and new systems under their purview, and that significant changes to the information system is documented in the system security plan per USDA Risk Management Framework (RMF) Guidelines.

(2) Ensure the system is deployed and operated according to the security controls.

(3) Establish system-level POAMs and implement corrective actions in accordance with the USDA POA&M Standard Operating Procedures.

(4) Identify and approve the General Users in conjunction with the Supervisor/Branch Chief for an IT business application. For Privileged Users, identify and determine their role in conjunction with the Supervisor/ISSO for IT business applications.

(5) Notify the ISSM/ISSO of any suspected incidents in a timely manner, and assist in the investigation of incidents, if necessary.

(6) Ensure personnel for the system are properly designated, monitored, and trained, including the appointment, in writing, of an individual to serve as the ISSO.

(7) Ensure system data is kept up-to-date using the FISMA security management toolset.

(8) Manage the risk posture for all systems for which they are designated systems owners.

(9) Ensure the systems that contain Classified, Confidential Business Information (CBI), and/or Controlled Unclassified Information (CUI), are managed effectively to prevent unauthorized disclosure and modification to the data. Ensure that all personnel having responsibility for PII or for activities that involve PII have completed the USDA PII training and ensure that the personnel certify acceptance of their responsibility for privacy requirements (activities to include the identification, labeling and safeguarding of data).

(10) Routinely meet with the ISSPM/representative and the ISSM to ensure that the A&A and POA&M remediation is being conducted.

(11) Ensure that all users (MRP employees, contractors and affiliates) are trained every fiscal year for all security training.

l. The MRP ISSM will:

(1) Be a full-time federal employee appointed by the MRP CISO.

(2) Be accountable to ISSPM for ensuring all security requirements are met for the MRP systems and applications. Specifically, meet with the ISSPM quarterly to discuss the status of:

(a) Remediation status of all POAMS with special emphasis on late and high impact POAMs, if any.

(b) A&A status of the Program applications and systems. All A&A including annual assessments must be done in a timely manner in accordance with the work leveling plan submitted to the Department towards the beginning of each fiscal year in October.

(c) Communication of security awareness and specialized training by the MRP due date.

(d) Work with Business System Manager to ensure that privacy documents are completed.

(3) Serve as the principal advisor to the program's AO, and system owners on all matters involving the security of the program's applications and systems.

(4) Ensure that all A&A packages are maintained in CSAM for the use in performing required security monitoring activities and reporting.

(5) Perform certification duties in support of the Assistant CIO for MRP and ensure annual compliance reviews are conducted to verify that all systems have in place effective, quality security documentation.

(6) Conduct annual continuous monitoring of the ISSP to ensure effective implementation of, and compliance with, established policies, directives, and procedures.

(7) Establish an internal standard process to monitor, track, and close remedial actions required to mitigate risks in accordance with the MRP standard for POAMs and the FISMA security management toolset.

(8) Participate in the POAM planning process to create individual POAMs.

(9) Attend status meetings as established by the system owner and address open POAMs, annual assessments, and other action items.

(10) Assist the System Owner in ensuring those with privileged access are revoked in a timely manner (e.g., transfer, resignation, retirement, change of job description, etc.) -- immediately for an individual being separated for adverse reasons or just prior to notifying him/her of the pending action.

(11) Maintain the IT system inventory in accordance with the FISMA management toolset.

(12) Act as the program unit's central point of contact for all information security incidents and report incidents to the MRP ISSPM.

(13) Distribute, as necessary, information to system owners and others concerning risks and potential risks to systems.

(14) Participate as a voting member of the MRP ISSM Council, participate in special committees under the ISSM Council, and provide other support for the ISSM Council, as appropriate.

(15) Review all deliverables for compliance with all NIST, Departmental, and MRP guidelines.

(16) Assist the Business System Manager/IT Project Manager with Developmental systems so the defining, documenting and testing of all security plans and controls are conducted through the developmental phase and throughout the whole SDLC to include decommissioning/disposal.

m. The ISSO will:

(1) Work with the system owner and ISSM and ensures the appropriate operational security posture is maintained for an information system.

NOTE: Multiple information systems may be assigned to a single ISSO.

(2) Ensure the implementation of security protection controls and procedures that are documented in, or referenced by, the System Security Plan for each information system for which he/she is responsible.

(3) Assist the system owner and ISSM in ensuring that all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before being granted access to the information system.

(4) Assist the system owner, IT Project Manager, and ISSM in ensuring that each information system user understands his/her responsibility for the security of information systems and information.

(5) Maintain and annually update the plan documents and A&A package for each information system for which he/she is the ISSO.

(6) Ensure that the ISSM is notified when an information system is no longer needed or when changes are planned that might affect the authorization of the information system.

NOTE: The retirement process initially starts with the Portfolio Management Branch and once approved, the appropriate CSAM retirement process takes place.

(7) Participate with the ISSM in the A&A process.

(8) Participate in the POAM planning process to create individual POAMs.

(9) Communicate individual incident(s) and potential incident reports to the ISSM and initiate protective or corrective actions.

(10) Ensure that unauthorized personnel are not granted use of, or access to, the information system. Ensure no system interconnections are established without completion and authorization of Interconnection Security Agreement.

(11) Assist the ISSM with ensuring that employees have completed the mandatory USDA Information Security Awareness and Rules of Behavior training.

(12) Attend weekly status meetings as established by the system owner and address open POAMs, annual assessments, and other action items; and provide feedback to Lessons Learned documents after every A&A project.

(13) Ensure that all new and legacy systems that are being enhanced have Secure Code Testing performed prior to the deployment into production systems.

n. The IT Project Manager will:

(1) Work with the Business System Manager, System Owner and ISSM to coordinate all activities that comprise a system's lifecycle from design through implementation.

(2) Assist with ensuring that A&A tasks include costs into the project schedule and budget A&A costs for both the development and maintenance stages of the project in alignment with the Capital Planning and Investment Control process.

(3) Coordinate and manage POAMs with the various subject matter experts who own and use the system.

(4) Ensure that all vulnerabilities are remediated within the system.

(5) Ensure that all new and legacy systems that are being enhanced have Secure Code Testing performed prior to deployment in production.

o. The System/Network Administrator's role may include security of local area network or application administration. As required, the system/network administrator will:

(1) Assist in the development and maintenance of system security plans and contingency plans for all systems under his/her responsibility.

(2) Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies.

(3) Participate in self-assessments of system safeguards, program elements, and A&A of the system.

(4) Evaluate proposed technical security controls to ensure proper integration with other system operations.

(5) Identify requirements for resources needed to effectively implement technical security controls.

(6) Ensure the integrity of the implementation and operation of technical security controls by conducting control security tests and evaluations.

(7) Develop SOPs, and manuals as directed by the system owner.

(8) Evaluate and develop procedures to ensure proper integration of service continuity with other system operations.

(9) Notify the responsible system owner or ISSM/ISSO of any suspected incidents in a timely manner, and assist in the investigation of incidents, if necessary.

(10) Once an account has been approved by the System Owner, the System Administrator will create the account within the business application.

p. Application Developers are responsible for developing applications. All applications must be developed in accordance with FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. The Application Developers will:

(1) Ensure that security controls are embedded into the system during the System Development Lifecycle process.

(2) Assist the system owner with developing security controls that relate to the application.

(3) Develop the automated mechanisms to implement the security controls.

(4) Develop protection that prohibits or limits the effects of denial of service attacks. Complete a test plan and ensure that testing is performed on new development prior to production release.

(5) Assist in the continuous monitoring that is a part of the A&A process.

(6) Ensure that all vulnerabilities are remediated within the system.

(7) Ensure that all new and legacy systems that are being enhanced have Secure Code Testing performed and identified vulnerabilities are remediated prior to deployment in production.

q. Procurement Personnel will ensure all IT contracts, Statement of Objectives (SOO), and Statement of Work (SOW) have specifically and adequately addressed the Federal Acquisitions Process, MRP ISSP, USDA Departmental Regulations, Privacy Act clauses, Records Management requirements, and the NIST guidelines in their language and implementation. They will:

(1) Advise all key MRP personnel of any procurement regulation changes that can affect the ISSP.

(2) Ensure that all necessary security clauses are included in all Government contracts.

(3) Ensure all IT contracts, SOO, and SOW are approved and meet the needs of a system and the business system manager.

r. MRP Human Resources Personnel will implement policy and procedures to ensure personnel security is covered. They will:

(1) Advise the MRP ISSPM of any personnel regulation changes that can affect the ISSP.

(2) Ensure on-boarding employees, students, contractors, volunteers, and other identified individuals complete annual security awareness and rules of behavior training.

(3) Ensure adequate employee off-boarding paperwork is processed and MRP-IT is notified to disable network access.

s. All MRP Users will comply with all Federal, USDA, and MRP-IT security requirements pertaining to the information resources they use. They will:

a. Take all mandatory information security training: Information Security Awareness (ISA) training; Privacy training, etc.

b. Report any cybersecurity incidents to MCIRT.

c. Abide by the Rules of Behavior as defined in the fiscal year ISA training.

8. RECORDS MANAGEMENT

Federal records created by this Directive must be maintained in accordance with the established General Records Schedule (GRS) and/or the APHIS/AMS Records Management Handbook when applicable. If employees are named in an active litigation hold, Freedom of Information Act (FOIA) request, and/or other action, those records, regardless of media, must be preserved and maintained in their native format until otherwise notified by your Agency Records Officer and/or the Office of General Counsel.

a. The System Owner (Agency Program) is the official record keeper of the following:

(1) System Security Plan (SSP)

(2) Contingency Plan (CP)

(3) Disaster Recovery Plan (DRP)

(4) Configuration Management Plan (CMP)

(5) Business Impact Analysis (BIA)

(6) Interconnection Service Agreement (ISA)

(7) Memorandum of Understanding (MOU)

(8) Privacy Threshold Analysis (PTA)

(9) Privacy Impact Assessment (PIA); *if needed*

(10) Plan of Action and Milestones (POA&M)

(11) Authorization to Operate (ATO) memo

The above records are permanently maintained in the USDA Cyber Security Assessment Management (CSAM) toolset.

b. The Chief Information Security Officer (CISO) is the official record keeper of the following:

(1) ISSM Appointment Memo

The ISSM Appointment memo is maintained in the CSSD I-drive under the ISSM Appointment memo folder. The record will be destroyed from the folder once a new ISSM has been appointed.

APHIS Records Management Handbook: ADM 4-3 Delegation of Authority: Disposition Authority NC1-310-77-2 - Temporary Destroy 10 years after delegation is cancelled.

(2) Workload Leveling Plan (WLP)

For MRP-IT, the WLP is maintained in the CSSD I-drive under the Fiscal Year Workload Leveling Plan folder.

The record will be destroyed once the next New Year begins with a new WLP. GRS 5.1 – Common Office Records, item #010. Disposition: Temporary: Destroy when business use ceases (end of the fiscal year). Disposition Authority: DAA-GRS-2016-0016-0001.

9. INQUIRIES AND ADDITIONAL INFORMATION

a. Direct inquiries or requests for changes to this Directive to the MRP ISSPM, located at 4700 River Road, Unit 103, Riverdale, MD 20737 or email to CSSD.Security.Management.Team@usda.gov.

b. For records management inquiries contact your Program Records Management Liaison for AMS/APHIS.

c. This Directive can be accessed online on the APHIS/AMS Directive homepages.

/s/
Joseph Stenaka
Acting Assistant CIO
MRP Information Technology