

U.S. DEPARTMENT OF AGRICULTURE  
WASHINGTON, D.C. 20250

|                                                                                             |                                  |
|---------------------------------------------------------------------------------------------|----------------------------------|
| <b>DEPARTMENTAL REGULATION</b>                                                              | NUMBER:<br>DR 3540-004           |
| SUBJECT: Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) | DATE:<br>May 30, 2023            |
| OPI: Office of the Chief Information Officer, Information Security Center                   | EXPIRATION DATE:<br>May 30, 2028 |

| <u>Section</u>                                          | <u>Page</u> |
|---------------------------------------------------------|-------------|
| 1. Purpose                                              | 1           |
| 2. Scope                                                | 2           |
| 3. Special Instructions/Cancellations                   | 3           |
| 4. Background                                           | 3           |
| 5. Policy                                               | 3           |
| 6. Roles and Responsibilities                           | 5           |
| 7. Penalties and Disciplinary Actions for Noncompliance | 7           |
| 8. Policy Exceptions                                    | 7           |
| 9. Inquiries                                            | 8           |
| Appendix A – Acronyms and Abbreviations                 | A-1         |
| Appendix B – Definitions                                | B-1         |
| Appendix C – Authorities and References                 | C-1         |

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the policy on managing information and communication technology (ICT) supply chain risks for the United States Department of Agriculture (USDA). It guides all Mission Areas, agencies, and staff offices to implement ICT supply chain risk management (SCRM). SCRM can consist of processes, personnel, and tools.
- b. To ensure that USDA complies with Federal requirements to manage ICT supply chain risks, this DR meets the requirements of:
  - (1) [Executive Order \(E.O.\) 14017](#), *America's Supply Chains*;
  - (2) [E.O. 14028](#), *Improving the Nation's Cybersecurity*;

- (3) *John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA)*, [Public Law \(P.L.\) 115-232](#);
- (4) *Federal Acquisition Regulation (FAR)*, [48 Code of Federal Regulations \(CFR\), Subpart 504.70](#), *Cyber-Supply Chain Risk Management*;
- (5) Office of Management and Budget (OMB) [M-22-18](#), *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*;
- (6) The National Institute of Standards and Technology (NIST) [Special Publication \(SP\) 800-37](#), Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*;
- (7) NIST [SP 800-53](#), Revision 5, *Security and Privacy Controls for Information Systems and Organizations*; and
- (8) NIST [SP 800-161](#), Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.

## 2. SCOPE

### a. This DR applies to the following:

- (1) All USDA Mission Areas, agencies, and staff offices;
- (2) Personnel who work for, or on behalf of, the USDA and are involved in SCRM in the acquisition of information technology (IT) products, components, or services;
- (3) All ICT investments, including major investments as defined in [DR 3130-008](#), *Definition of Major Information Technology Investments*; non-major IT investments as defined in [DR 3130-009](#), *Non-Major Information Technology (IT) Investments*; and micro-purchases used or operated by, for, or on behalf of USDA; and
- (4) Facilities from which these systems or services operate, whether owned or operated by USDA. This includes third parties operating on behalf of USDA by a contractor, subcontractor, or other organization.

### b. Nothing in this policy alters the requirements for protecting national security systems or information. This includes those identified in the [Federal Information Security Modernization Act of 2014 \(FISMA\)](#) and the [Committee on National Security Systems \(CNSS\)](#) policies, directives, instructions, and standards, and intelligence community policies, directives, and instructions.

### 3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This DR is effective immediately when published and will remain in effect until superseded or expiration.
- b. All USDA Mission Areas, agencies, and staff offices will align their related SCRM policies with this DR within 6 months of the publication date.
- c. The term “USDA personnel” encompasses USDA employees, appointees, contractors, partners, interns, fellows, affiliates, and volunteers.

### 4. BACKGROUND

- a. Technology solutions provided through a supply chain of competing vendors offer significant benefits to the Mission Area, agency, or staff office. They include low cost, interoperability, rapid innovation, and product feature variety. The ease of acquiring either technology or the lower costs, or both, are some of the benefits focused on in supply management. Unfortunately, these benefits also come with additional risks. The risks, which inherently come with the benefits, are easy to forget.
- b. Cybersecurity risks exist throughout the supply chain. They often go undetected and impact both the supplier and the end user. Vulnerabilities in the supply chain are often interconnected. They may expose enterprises to cascading cybersecurity risks. The non-standardized nature of ICT SCRM practices adds an additional layer of complexity. ICT SCRM is the organized and purposeful management of cybersecurity risks throughout the supply chain.

### 5. POLICY

- a. It is USDA policy to secure and protect the ICT supply chain from known threats. This policy is consistent with E.O. 14017, the FAR, OMB, and NIST standards. Known threats against USDA within the ICT supply chain include, but are not limited to:
  - (1) Insertion of counterfeit components;
  - (2) Malicious software; and
  - (3) Unauthorized production, tampering, theft, and poor manufacturing.
- b. The Office of the Chief Information Officer (OCIO), Information Security Center (ISC) will provide ICT SCRM governance, and will:
  - (1) Maintain oversight of the ICT SCRM process;

- (2) Conduct Departmentwide ICT SCRM assessments of existing suppliers;
  - (3) Conduct ICT SCRM assessments of potential suppliers during the cybersecurity technical review of the [Acquisition Approval Request \(AAR\)](#) process for security and compliance with:
    - (a) [DR 3130-010](#), *United States Department of Agriculture Enterprise Information Technology Governance*;
    - (b) [DR 3130-013](#), *Information Technology Capital Planning and Investment Control*; and
    - (c) [DR 3145-001](#), *Oversight and Management of the Federal Information Technology Acquisition Reform Act (FITARA)*;
  - (4) Tailor the inclusion of ICT SCRM requirements in contract language;
  - (5) Implement procedures and processes to detect counterfeit and compromised ICT products prior to deployment; and
  - (6) Document provenance and ensure compliance with applicable Federal laws, policies, and regulations (i.e., NDAA Section 889, E.O. 14017, and the Department of Commerce, Bureau of Industry and Security (BIS) [Supplement No. 4 to Part 744 – Entity List](#)).
- c. Each Mission Area, agency, and staff office will:
- (1) Align ICT SCRM practices with the [USDA Cybersecurity Supply Chain Implementation Plan \(I-Plan\)](#);
  - (2) Meet applicable contract requirements regarding ICT SCRM governance (i.e., FAR);
  - (3) Follow ICT SCRM best practices and applicable policies to reduce overall supply chain risk to an acceptable level;
  - (4) Prevent ICT suppliers from introducing risk to ICT systems that support the agricultural community;
  - (5) Require ICT suppliers to provide documentation that communicates assurance practices to assist in making informed risk-based decisions;
  - (6) Include critical software SCRM measures in accordance with E.O. 14028 and NIST [SP 800-218](#), *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*;

- (7) Document and analyze lessons learned in relation to ICT SCRM. All USDA Mission Areas, agencies, and staff offices will use this objective and subjective data to assess and improve the effectiveness of their programs and practices, and to control activities, procedures, and tasks; and
- (8) USDA Mission Areas, agencies, and staff offices will document and analyze lessons learned on their programs, control activities, procedures, and tasks. They will use this qualitative and quantitative data to assess effectiveness and to guide process improvement.

## 6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) will:
  - (1) Ensure that USDA complies with all Federal guidance related to SCRM;
  - (2) Oversee activities to manage information security and privacy programs. Ensure that controls are implemented correctly. The activities must be operating as intended. All activities must meet the requirements;
  - (3) Collaborate with the Director, Office of Budget and Program Analysis (OBPA), who serves as the Chief Risk Officer (CRO) and Senior Agency Official for Risk Management (SAORM) to ensure that ICT SCRM is integrated into Enterprise Risk Management (ERM); and
  - (4) Approve or delegate the approval to quarantine or remove ICT products or contract support services.
- b. The USDA Chief Information Security Officer (CISO) will:
  - (1) Oversee implementation of the Departmentwide ICT SCRM program;
  - (2) Appoint the Director of the Security Management Division (SMD) within OCIO ISC to maintain an effective ICT SCRM program;
  - (3) Collaborate with internal and external stakeholders to facilitate ICT SCRM compliance;
  - (4) Advise the CIO on risk recommendations to quarantine or remove ICT products or contract support services; and
  - (5) Approve enterprise risk-based decisions for ICT products and services.
- c. The Director, OBPA, serving as the CRO and SAORM, will establish and oversee a process for ERM.

- d. The General Counsel will provide guidance regarding the legality of ICT SCRM Implementation Plan (I-Plan) processes.
- e. The Director of the Office of Contracting and Procurement (OCP) will:
  - (1) Ensure that USDA complies with applicable contracting laws, policies, and regulations;
  - (2) Ensure that all USDA contracts comply with the FAR, the [\*USDA Cyber Supply Chain Risk Management \(C-SCRM\) Contract Language\*](#) guidance; and
  - (3) Facilitate ICT SCRM appeal processes.
- f. Mission Area Assistant CIOs will:
  - (1) Coordinate FAR and other contract-related activities or requirements with the OCP Director; and
  - (2) Ensure that requirements in this DR are implemented across their Mission Areas, agencies, and staff offices as appropriate.
- g. The Director of the OCIO ISC SMD will:
  - (1) Review and approve all ICT SCRM mitigation plans and associated Plan of Action and Milestones (POA&M);
  - (2) Assess the effectiveness and efficiency of the ICT SCRM program capabilities;
  - (3) Establish the criteria for the ICT SCRM risk-based decisions;
  - (4) Provide risk recommendations to the CISO to deny, quarantine, or remove ICT products and contract support services;
  - (5) Serve as a technical subject matter expert for policies and processes that govern USDA ICT SCRM activities;
  - (6) Develop, maintain, and communicate the [\*USDA Certified Software List\*](#); and
  - (7) Oversee the cybersecurity technical review of ICT SCRM activities under the AAR process and ICT Supply Chain Assessments.
- h. OCIO ISC ICT SCRM Analysts will:
  - (1) Conduct ICT SCRM risk assessments; and

- (2) Communicate all pertinent ICT SCRM information through the appropriate channels to the SMD Director.
- i. Authorizing Officials (AO) will:
  - (1) Ensure the implementation of USDA ICT SCRM I-Plan, approve mitigation plans, and issue risk-based decisions for systems within their purview; and
  - (2) Document ICT SCRM system activities in the System of Record as required.
- j. Mission Area SCRM Points of Contact will:
  - (1) Serve as Mission Area liaisons to the OCIO ICT SCRM team; and
  - (2) Communicate all pertinent ICT SCRM information to OCIO.

## 7. PENALTIES AND DISCIPLINARY ACTIONS FOR NONCOMPLIANCE

USDA established personnel responsibilities and acceptable conduct regarding the use of computers and telecommunications equipment in [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16, *Computers*. In addition, DR 4070-735-001, Section 21, *Disciplinary or Adverse Action* states:

- a. Any violation of the responsibilities or standards contained in this DR may be cause for disciplinary or adverse action; and
- b. Any disciplinary or adverse action taken will be consistent with the applicable laws and regulations.

## 8. POLICY EXCEPTIONS

- a. All Mission Areas, agencies, and staff offices must conform to this policy. If necessary, they may request a policy exception via the risk-based decision process. An approved risk-based decision is an acceptance of risk but does not constitute compliance with policy. Requests for a policy exception must include:
  - (1) Acknowledge the noncompliance with policy;
  - (2) Document an acceptable plan to remediate the weakness, as indicated in the [POA&M-SOP-3540-003A](#), *Standard Operating Procedures (SOP) on Plan of Action & Milestones (POA&M) Management*.

- b. Submit policy exception requests to the Mission Area AO in accordance with [RBD-SOP-3540-003B](#), *USDA Standard Operating Procedures on Risk-Based Decision Management*.

## 9. INQUIRIES

Send any questions or concerns about this DR to the OCIO, ISC, via [SMD-PCB-Policy@usda.gov](mailto:SMD-PCB-Policy@usda.gov).

-END-

## APPENDIX A

### ACRONYMS AND ABBREVIATIONS

|        |                                                                                       |
|--------|---------------------------------------------------------------------------------------|
| AAR    | Acquisition Approval Request                                                          |
| AO     | Authorizing Official                                                                  |
| BIS    | Bureau of Industry and Security                                                       |
| C-SCRM | Cyber Supply Chain Risk Management                                                    |
| CFR    | Code of Federal Regulations                                                           |
| CIO    | Chief Information Officer                                                             |
| CISO   | Chief Information Security Officer                                                    |
| CNSS   | Committee on National Security Systems                                                |
| CNSSI  | Committee on National Security Systems Instruction                                    |
| CPITGD | Capital Planning and Information Technology Governance Division (OCIO-IRMC component) |
| CRO    | Chief Risk Officer                                                                    |
| DN     | Departmental Notice                                                                   |
| DR     | Departmental Regulation                                                               |
| E.O.   | Executive Order                                                                       |
| ERM    | Enterprise Risk Management                                                            |
| FAR    | Federal Acquisition Regulation                                                        |
| FISMA  | Federal Information Security Modernization Act of 2014                                |
| FITARA | Federal Information Technology Acquisition Reform Act                                 |
| I-PLAN | Implementation Plan                                                                   |
| ICT    | Information and Communication Technology                                              |
| IRMC   | Information Resource Management Center (OCIO component)                               |
| ISC    | Information Security Center (OCIO component)                                          |
| IT     | Information Technology                                                                |
| NDAA   | John S. McCain National Defense Authorization Act for Fiscal Year 2019                |
| NIST   | National Institute of Standards and Technology                                        |
| OBPA   | Office of Budget and Program Analysis                                                 |
| OCIO   | Office of the Chief Information Officer                                               |
| OCP    | Office of Contracting and Procurement                                                 |
| OMB    | Office of Management and Budget                                                       |
| P.L.   | Public Law                                                                            |
| POA&M  | Plan of Action and Milestones                                                         |
| SAORM  | Senior Agency Official for Risk Management                                            |
| SCRM   | Supply Chain Risk Management                                                          |
| SMD    | Security Management Division (OCIO-ISC component)                                     |
| SOP    | Standard Operating Procedures                                                         |
| SP     | Special Publication                                                                   |
| SSDF   | Secure Software Development Framework                                                 |
| U.S.C. | United States Code                                                                    |
| USDA   | United States Department of Agriculture                                               |

## APPENDIX B

### DEFINITIONS

Micro-Purchases. An acquisition of supplies or services using simplified acquisition procedures, the aggregate amount of which does not exceed the micro-purchase threshold. (Source: FAR Part 2)

Information and Communication Technology (ICT). Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information. (Source: NIST, [Glossary](#))

Supply Chain Risk Management (SCRM). The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. (Source: NIST, *Glossary*)

## APPENDIX C

### AUTHORITIES AND REFERENCES

CNSS, [CNSS Instruction \(CNSSI\) - 4009](#), *Committee on National Security Systems Glossary*, March 2, 2022

CNSS, [Introducing the CNSS Library](#) website

Department of Commerce, BIS, [Supplement No. 4 to Part 744 – Entity List](#), April 12, 2023

[E.O. 14017](#), *America’s Supply Chains*, February 24, 2021

[E.O. 14028](#), *Improving the Nation’s Cybersecurity*, May 12, 2021

*Federal Acquisition Regulation (FAR)*, [48 CFR Subpart 504.70](#), *Cyber Supply Chain Risk Management*, as amended

FAR, [48 CFR Part 2](#), *Definitions of Words and Terms*

*Federal Agency Responsibilities*, [44 United States Code \(U.S.C.\) § 3506](#)

*Federal Information Security Modernization Act of 2014 (FISMA)*, [P.L. 113-283](#), December 18, 2014

General Services Administration, *Cybersecurity Supply Chain Risk Management Guide (C-SCRM)* Version 1.0, May 2022, as amended

*John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA)*, [P.L. 115-232](#), August 13, 2018

NIST, Computer Security Resource Center, [Glossary](#)

NIST, [SP 800-37](#), Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018, as amended

NIST, [SP 800-53](#), Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of December 10, 2020, as amended

NIST, [SP 800-161](#), Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, May 2022, as amended

NIST, [SP 800-218](#), *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*, February 2022, as amended

Office of Government Ethics, [5 CFR § 2635, et seq.](#), *Standards of Ethical Conduct for Employees of the Executive Branch*

OMB, [M-22-18](#), *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, September 14, 2022

*Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act*, [P.L. 115-390](#), December 21, 2018, as amended

USDA, [DR 3130-008](#), *Definition of Major Information Technology Investments*, August 13, 2020

USDA, [DR 3130-009](#), *Non-Major Information Technology (IT) Investments*, September 28, 2020

USDA, [DR 3130-010](#), *United States Department of Agriculture Enterprise Information Technology Governance*, April 20, 2021

USDA, [DR 3130-013](#), *Information Technology Capital Planning and Investment Control*, May 24, 2021

USDA, [DR 3145-001](#), *Oversight and Management of the Federal Information Technology Acquisition Reform Act (FITARA)*, May 7, 2021

USDA, [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, October 4, 2007

USDA, OCIO, Information Resource Management Center (IRMC), Capital Planning and Information Technology Governance Division (CPITGD), [Acquisition Approval Request \(AAR\) Guidance for AAR Managers](#), Version 2.5, August 2022

USDA, [POA&M-SOP-3540-003A](#), *Standard Operating Procedures (SOP) on Plan of Action & Milestones (POA&M) Management*, Version 1.3, September 17, 2021

USDA, [RBD-SOP-3540-003B](#), *USDA Standard Operating Procedures on Risk-Based Decision Management*, Revision 1.6, September 17, 2021

USDA, [USDA Certified Software List](#)

USDA, [USDA Cybersecurity Supply Chain Implementation Plan \(I-Plan\)](#), Version 1.0, March 16, 2022

USDA, [USDA Cyber Supply Chain Risk Management \(C-SCRM\) Contract Language](#), Version 1.0, November 4, 2020