Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028

July 9, 2021

Introduction

Executive Order (EO) 14028 on Improving the Nation's Cybersecurity, May 12, 2021, directs the National Institute of Standards and Technology (NIST) to publish guidance on security measures for EO-critical software use, based on the definition of "EO-critical software" NIST developed for the EO.

> *(i) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Homeland Security acting through the Director of CISA and with the Director of OMB, shall publish guidance outlining security measures for critical software as defined in subsection (g) of this section, including applying practices of least privilege, network segmentation, and proper configuration.*

The EO directs the Office of Management and Budget (OMB) to require agencies to comply with the security measures guidance.

> *(j) Within 30 days of the issuance of the guidance described in subsection (i) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidance.*

To help identify and prioritize possible security measures for inclusion, NIST solicited position papers from the community, hosted a virtual workshop to gather input, consulted with the Cybersecurity & Infrastructure Security Agency (CISA) and OMB, and reviewed existing federal guidance on individual security measures that might apply to EO-critical software use.

This document starts with information about the purpose and scope of the guidance, including the meaning of "EO-critical software use." Next, it defines the fundamental security measures for EO-critical software use. It concludes with Frequently Asked Questions (FAQ) that provide additional information on the guidance and its relationship to other tasks in the EO and to other federal cybersecurity initiatives. The last item in the FAQ is a summary of the security measures.

Guidance Purpose and Scope

Recent incidents have demonstrated the need to better protect the EO-critical software that federal agencies use on-premises, in the cloud, and elsewhere to achieve their missions. Even though EO-critical software may be developed using recommended secure development practices, it still needs to be secured in operational environments. There is increasing recognition that all organizations should assume that a breach is going to occur or has already occurred, so access to EO-critical software must be limited at all times to only what is needed. Moreover, there must be constant monitoring for anomalous or malicious activity. Preventing breaches is still a "must," but it is also important to have robust incident detection, response, and recovery capabilities. Such capabilities can help identify breaches, determine their scope of impact, discover root causes, and restore normal operations quickly, thus minimizing disruption to agency missions.

The scope of this guidance on security measures is federal agency **use** of EO-critical software. **Development and acquisition** of EO-critical software **are out of scope**. The security measures are intended to protect the use of deployed EO-critical software in agencies' operational environments.

NIST defined the following objectives for the security measures:

1. Protect EO-critical software and *EO-critical software platforms* (the platforms on which EO-critical software runs, such as endpoints, servers, and cloud resources) from unauthorized access and usage.
2. Protect the confidentiality, integrity, and availability of data used by EO-critical software and EO-critical software platforms. (See FAQ #6.)
3. Identify and maintain EO-critical software platforms and the software deployed to those platforms to protect the EO-critical software from exploitation.
4. Quickly detect, respond to, and recover from threats and incidents involving EO-critical software and EO-critical software platforms.
5. Strengthen the understanding and performance of humans' actions that foster the security of EO-critical software and EO-critical software platforms.

NIST has identified security measures that are fundamental for meeting these objectives. These "Security Measures for EO-Critical Software Use" are not intended to be comprehensive, nor are they intended to eliminate the need for other security measures that federal agencies implement as part of their existing requirements and cybersecurity programs. Agencies should continue their efforts to secure systems and networks that EO-critical software runs on and to manage cyber supply chain risk (see FAQ #4), as well as implement zero trust practices (see FAQ #5), which depend on the fundamental security measures. The intent of specifying these security measures is to assist agencies by defining a set of common security objectives for prioritizing the security measures that should be in place to protect EO-critical software use.

Security Measures for EO-Critical Software Use

The table below defines the security measures for EO-critical software use. The security measures are grouped by objective. The columns in the table are:

- **Security Measure (SM)**: A high-level security outcome statement that is intended to apply to all software designated as EO-critical software or to all platforms, users, administrators, data, or networks (as specified) that are part of running EO-critical software.
- **Federal Government Informative References:** Federal Government-issued publications and projects that, in whole or in part, discuss the security measure. The first two references for each security measure are the NIST Cybersecurity Framework and NIST Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations. These two references list their mappings to the security measure (as Cybersecurity Framework Subcategories and SP 800-53 security controls, respectively). These mappings are general and informational; any particular situation might have somewhat different mappings.

  All references after the first two are selected examples that discuss or illustrate the security measure and are intended as possible sources of information. Some references only apply to

particular use cases, environments, situations, etc. Omission from this list does not imply that other sources of information should not be used.

The references listed in the table will be updated periodically as new publications are identified or released, and as existing publications are updated.

The acronyms used in the table are:

- **CISA:** Cybersecurity & Infrastructure Security Agency
- **DISA:** Defense Information Systems Agency
- **GSA**: General Services Administration
- **NIST**: National Institute of Standards and Technology
- **NSA**: National Security Agency
- **OMB**: Office of Management and Budget

Security Measure (SM)	Federal Government Informative References
Objective 1: Protect EO-critical software and EO-critical software platforms from unauthorized access and usage.	
SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms. (See FAQ #7.)	▪ **NIST,** Cybersecurity Framework: PR.AC-1, PR.AC-7 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AC-2, IA-2, IA-4, IA-5 ▪ **CISA,** Bad Practices ▪ **CISA**, Capacity Enhancement Guide: Implementing Strong Authentication ▪ **CISA**, CDM Program Dashboard Ecosystem ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Identity and Access Management – Who is on the Network? ▪ **GSA**, Federal Identity, Credential, and Access Management (FICAM) Architecture ▪ **GSA**, IDManagement.gov ▪ **NIST**, Best Practices for Privileged User PIV Authentication ▪ **NIST,** SP 800-63-3, Digital Identity Guidelines ▪ **NIST,** SP 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials ▪ **NIST,** SP 1800-12, Derived Personal Identity Verification (PIV) Credentials ▪ **NIST**, SP 1800-17, Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers ▪ **NSA,** Selecting Secure Multi-factor Authentication Solutions ▪ **NSA,** Transition to Multi-Factor Authentication ▪ **OMB,** Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management

Security Measure (SM)	Federal Government Informative References
SM 1.2: Uniquely identify and authenticate each service attempting to access EO-critical software or EO-critical software platforms.	▪ **NIST,** Cybersecurity Framework**:** PR.AC-1, PR.AC-7 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AC-2, IA-9 ▪ **CISA,** Bad Practices
SM 1.3: Follow privileged access management principles for network-based administration of EO-critical software and EO-critical software platforms. Examples of possible implementations include using hardened platforms dedicated to administration and verified before each use, requiring unique identification of each administrator, and proxying and logging all administrative sessions to EO-critical software platforms.	▪ **NIST,** Cybersecurity Framework**:** PR.AC-1, PR.AC-7, PR.MA-1, PR.MA-2 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AC-2, IA-2, SC-2, SC-7 enhancement 15 ▪ **CISA**, Securing High Value Assets ▪ **CISA**, Securing Network Infrastructure Devices
SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data. Examples of such techniques include network segmentation, isolation, software-defined perimeters, and proxies.	▪ **NIST,** Cybersecurity Framework**:** PR.AC-3, PR.AC-5 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: SC-7 ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Network Security Management – What is Happening on the Network? How is the Network Protected? ▪ **CISA,** Defending Against Software Supply Chain Attacks ▪ **CISA**, Securing Network Infrastructure Devices ▪ **CISA**, Trusted Internet Connections 3.0: Traditional TIC Use Case ▪ **NIST,** SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy ▪ **NIST,** SP 800-207, Zero Trust Architecture ▪ **NSA,** Segment Networks and Deploy Application-Aware Defenses

Security Measure (SM)	Federal Government Informative References
Objective 2: Protect the confidentiality, integrity, and availability of data used by EO-critical software and EO-critical software platforms. (See FAQ #6.)	
SM 2.1: Establish and maintain a data inventory for EO-critical software and EO-critical software platforms.	▪ **NIST,** Cybersecurity Framework**:** ID.AM-3, DE.AE-1 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: CM-8, PM-5 ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Data Protection Management – How is Data Protected? ▪ **CISA,** Defending Against Software Supply Chain Attacks ▪ **CISA,** Software Asset Management FAQ ▪ **GSA,** Inventory.data.gov Guide ▪ **NIST,** Data Classification project ▪ **OMB**, Memorandum M-16-12, Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing
SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	▪ **NIST,** Cybersecurity Framework**:** PR.AC-4 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AC-2, AC-3, AC-6 ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Identity and Access Management – Who is on the Network? ▪ **CISA,** QSMO Services – Identity Management and Access Control ▪ **NIST,** SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations ▪ **NIST,** SP 800-205, Attribute Considerations for Access Control Systems ▪ **NIST,** SP 800-207, Zero Trust Architecture
SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	▪ **NIST,** Cybersecurity Framework**:** PR.DS-1 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: SC-28 ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Data Protection Management – How is Data Protected? ▪ **CISA,** Protecting Data on the Network with Multi-Layered Data Protection Strategies ▪ **NIST,** SP 800-111, Guide to Storage Encryption Technologies for End User Devices ▪ **NIST,** SP 800-175B Rev. 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms ▪ **NIST,** SP 800-209, Security Guidelines for Storage Infrastructure ▪ **OMB,** Circular A-130, Appendix I, 4. i. 14

Security Measure (SM)	Federal Government Informative References
SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	▪ **NIST,** Cybersecurity Framework**:** PR.AC-3, PR.AC-7, PR.DS-2, PR.PT-4, DE.CM-7 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AC-4, AC-17, SC-8 ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Data Protection Management – How is Data Protected? ▪ **CISA,** Protecting Data on the Network with Multi-Layered Data Protection Strategies ▪ **NIST,** SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security ▪ **NIST,** SP 800-47 Rev. 1, Managing the Security of Information Exchanges ▪ **NIST,** SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations ▪ **NIST,** SP 800-77 Rev. 1, Guide to IPsec VPNs ▪ **NIST,** SP 800-175B Rev. 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms ▪ **NSA,** Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations ▪ **OMB,** Circular A-130, Appendix I, 4. i. 14 ▪ **OMB,** Memorandum M-15-13, Policy to Require Secure Connections across Federal Websites and Web Services
SM 2.5: Back up data, exercise backup restoration, and be prepared to recover data used by EO-critical software and EO-critical software platforms at any time from backups.	▪ **NIST,** Cybersecurity Framework**:** PR.IP-4 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: CP-9, CP-10 ▪ **NIST,** SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems ▪ **NIST,** SP 800-57 Rev. 5, Recommendation for Key Management: Part 1—General ▪ **NIST,** SP 800-175B Rev. 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

Security Measure (SM)	Federal Government Informative References
Objective 3: Identify and maintain EO-critical software platforms and the software deployed to those platforms to protect the EO-critical software from exploitation.	
SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	▪ **NIST,** Cybersecurity Framework: ID.AM-1, ID.AM-2, ID.SC-2 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: CM-8, PM-5, RA-9 ▪ **CISA**, CDM Program Dashboard Ecosystem ▪ **CISA**, CDM Software Asset Management (SWAM) Capability ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Asset Management – What is on the Network? ▪ **CISA,** Defending Against Software Supply Chain Attacks ▪ **NIST,** IR 8011 Vol. 3, Automation Support for Security Control Assessments: Software Asset Management ▪ **NIST,** SP 1800-5, IT Asset Management
SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms. Practices include: ▪ rapidly identify, document, and mitigate known vulnerabilities (e.g., patching, updating, upgrading software to supported version) to continuously reduce the exposure time ▪ monitor the platforms and software to ensure the mitigations are not removed outside of change control processes	▪ **NIST,** Cybersecurity Framework**:** ID.RA-1, ID.RA-2, ID.RA-6, PR.IP-12, DE.CM-8, RS.MI-3 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: CA-7, RA-5, SI-2, SI-5, SR-8 ▪ **CISA,** Bad Practices ▪ **CISA,** Capacity Enhancement Guide: Remote Vulnerability and Patch Management ▪ **CISA**, CDM Program Dashboard Ecosystem ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Asset Management – What is on the Network? ▪ **CISA,** Defending Against Software Supply Chain Attacks ▪ **NIST,** IR 8011 Vol. 4, Automation Support for Security Control Assessments: Software Vulnerability Management ▪ **NIST**, Patching the Enterprise project ▪ **NIST,** SP 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies

Security Measure (SM)	Federal Government Informative References
SM 3.3: Use configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms. Practices include: ▪ identify the proper hardened security configuration for each EO-critical software platform and all software deployed to that platform (hardened security configurations enforce the principles of least privilege, separation of duties, and least functionality) ▪ implement the configurations for the platforms and software ▪ control and monitor the platforms and software to ensure the configuration is not changed outside of change control processes	▪ **NIST,** Cybersecurity Framework**:** ID.RA-1, ID.RA-2, ID.RA-6, PR.AC-4, PR.IP-1, PR.IP-3, PR.PT-3, DE.CM-8, RS.MI-3 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AC-5, AC-6, CA-7, CM-2, CM-3, CM-6, CM-7, RA-5, SI-5 ▪ **CISA**, CDM Program Dashboard Ecosystem ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Asset Management – What is on the Network? ▪ **CISA,** Defending Against Software Supply Chain Attacks ▪ **DISA,** STIGs Document Library ▪ **NIST**, National Checklist Program (NCP) Checklist Repository ▪ **NIST,** SP 800-70 Rev. 4, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers ▪ **NIST,** SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
Objective 4: Quickly detect, respond to, and recover from threats and incidents involving EO-critical software and EO-critical software platforms.	
SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	▪ **NIST,** Cybersecurity Framework**:** PR.PT-1 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12 ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Network Security Management – What is Happening on the Network? How is the Network Protected? ▪ **CISA,** Technical Approaches to Uncovering and Remediating Malicious Activity ▪ **NIST**, National Checklist Program (NCP) Checklist Repository ▪ **NIST,** SP 800-92, Guide to Computer Security Log Management ▪ **OMB,** Circular A-130, Appendix I, 4. i. 7

Security Measure (SM)	Federal Government Informative References
SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	▪ **NIST,** Cybersecurity Framework**:** DE.CM-7 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: CA-7, SI-4 ▪ **CISA,** Continuous Diagnostics and Mitigation (CDM) ▪ **CISA,** Defending Against Software Supply Chain Attacks ▪ **NIST,** IR 8011 Vol. 3, Automation Support for Security Control Assessments: Software Asset Management ▪ **NIST,** SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them. Capabilities include: ▪ protecting the software, data, and platform by identifying, reviewing, and minimizing the attack surface and exposure to known threats ▪ permitting only verified software to execute (e.g., file integrity verification, signed executables, allowlisting) ▪ proactively detecting threats and stopping them when possible ▪ responding to and recovering from incidents ▪ providing the necessary information for security operations, threat hunting, incident response, and other security needs	▪ **NIST,** Cybersecurity Framework**:** PR.DS-5, PR.DS-6, DE.AE-2, DE.CM-4, DE.CM-7, DE.DP-4 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: SI-3, SI-4, SI-7 ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Data Protection Management – How is Data Protected? ▪ **CISA,** Defending Against Software Supply Chain Attacks ▪ **NIST,** SP 800-61 Rev. 2, Computer Security Incident Handling Guide ▪ **NIST,** SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops ▪ **NIST,** SP 800-150, Guide to Cyber Threat Information Sharing ▪ **NIST,** SP 800-167, Guide to Application Whitelisting ▪ **NIST,** SP 800-184, Guide for Cybersecurity Event Recovery ▪ **NSA,** Enforce Signed Software Execution Policies

Security Measure (SM)	Federal Government Informative References
SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks. Capabilities include: ▪ proactively detecting threats at all layers of the stack, including the application layer, and stopping them when possible ▪ providing the necessary information for security operations, threat hunting, incident response, and other security needs	▪ **NIST,** Cybersecurity Framework**:** PR.DS-5, DE.AE-1, DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.DP-4 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AU-13, AU-14, SC-7, SI-3 ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Data Protection Management – How is Data Protected? ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Network Security Management – What is Happening on the Network? How is the Network Protected? ▪ **CISA,** Defending Against Software Supply Chain Attacks ▪ **CISA,** Securing Network Infrastructure Devices ▪ **CISA**, Trusted Internet Connections 3.0: Traditional TIC Use Case ▪ **NIST,** SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy ▪ **NIST,** SP 800-61 Rev. 2, Computer Security Incident Handling Guide ▪ **NIST,** SP 800-94 Rev. 1, Guide to Intrusion Detection and Prevention Systems (IDPS)
SM 4.5: Train all security operations personnel and incident response team members, based on their roles and responsibilities, on how to handle incidents involving EO-critical software or EO-critical software platforms.	▪ **NIST,** Cybersecurity Framework**:** PR.AT-5, PR.IP-9, PR.IP-10 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AT-3, CP-3, IR-2 ▪ **CISA,** Incident Response Training ▪ **NIST,** SP 800-61 Rev. 2, Computer Security Incident Handling Guide ▪ **NIST,** SP 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework)
Objective 5: Strengthen the understanding and performance of humans' actions that foster the security of EO-critical software and EO-critical software platforms.	
SM 5.1: Train all users of EO-critical software, based on their roles and responsibilities, on how to securely use the software and the EO-critical software platforms.	▪ **NIST,** Cybersecurity Framework**:** PR.AT-1 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AT-2, AT-3 ▪ **CISA,** PCII Authorized User Training ▪ **NIST,** SP 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework)
SM 5.2: Train all administrators of EO-critical software and EO-critical software platforms, based on their roles and responsibilities, on how to securely administer the software and/or platforms.	▪ **NIST,** Cybersecurity Framework**:** PR.AT-2 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AT-3, CP-3 ▪ **NIST,** SP 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework)

Security Measure (SM)	Federal Government Informative References
SM 5.3: Conduct frequent awareness activities to reinforce the training for all users and administrators of EO-critical software and platforms, and to measure the training's effectiveness for continuous improvement purposes.	▪ **NIST,** Cybersecurity Framework**:** PR.AT-1, PR.AT-2 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: AT-3 ▪ **CISA,** Cyber Education and Awareness ▪ **NIST,** SP 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework)

FAQs

The following FAQs provide additional information on the guidance.

1. **Are all of the security measures appropriate for all EO-critical software?**

   A security measure might not be relevant for a particular situation based on the nature of the software deployment or other factors. If a particular security measure cannot be implemented, other security measures could be identified and implemented to mitigate the risk and achieve the outcome that the missing security measure was intended to address. Agencies are still expected to apply risk management activities as part of their overall cybersecurity programs.

2. **Will this guidance be updated as more types of EO-critical software are identified?**

   Potentially. However, all of the security measures for EO-critical software are anticipated to apply to all types of EO-critical software in all deployments.

3. **How can we implement the security measures for using cloud-based EO-critical software?**

   CISA, GSA's FedRAMP program, and OMB are currently developing a federal cloud-security strategy and cloud-security technical reference architecture documentation in support of Section 3 of the EO. The security measures for using EO-critical software could be applied to cloud-based environments by cloud service providers.

4. **Does NIST have additional resources on cyber supply chain risk management (C-SCRM)?**

   Yes, see NIST's C-SCRM project website for links to all the resources. An example is the Federal C-SCRM Forum, which NIST hosts; the Forum fosters collaboration and the exchange of C-SCRM information among federal agencies to improve the security of federal supply chains. Examples of NIST C-SCRM guidance include SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations and SP 800-161 Rev. 1 (Draft), Cyber Supply Chain Risk Management Practices for Systems and Organizations.

5. **What is the relationship between this guidance and zero trust architecture?**

   Section 3 of the EO directs each federal agency to plan to implement zero trust architecture. All of the security measures for EO-critical software defined in this guidance are also components of a zero trust architecture, although by no means are they complete. Agencies developing plans for migrating to zero trust architecture can incorporate the security measures for EO-critical software use into those plans. For more information on zero trust architecture, see the following Federal Government resources:

- *DISA and NSA, Department of Defense (DOD) Zero Trust Reference Architecture Version 1.0*
- *NIST, SP 800-207, Zero Trust Architecture*
- *NSA, Embracing a Zero Trust Security Model*

6. **Objective 2 says to "protect the confidentiality, integrity, and availability of data," but what about cases where not all three of those are needed, like protecting the confidentiality of publicly available information?**

   Agencies should continue to take risk-based approaches for protecting data, and thus should only apply the types of protection that will reduce risk for a particular scenario. For example, protecting the confidentiality of publicly available information typically will not reduce risk, and thus would not be necessary.

7. **SM 1.1 includes the term "verifier impersonation-resistant." What does that mean?**

   Verifier impersonation-resistant authentication protocols and credentials ensure that when a user or administrator attempts to connect to EO-critical software or an EO-critical software platform over a network, both parties (the person and the platform) are legitimate. Verifier impersonation resistance helps prevent people from having their credentials stolen by phishing attacks, and also helps prevent attackers from using stolen authentication information to impersonate a user or administrator. There are several ways to achieve verifier impersonation resistance; an example of a verifier impersonation-resistant protocol is client-authenticated Transport Layer Security (TLS). See Section 5.2.5 of NIST SP 800-63B for more information.

8. **Where can I learn more about EO-critical software?**

   Additional information is available at this webpage. It includes a set of FAQs that provide more details and context about EO-critical software.

9. **Is there a summary of the security measures?**

   Yes, the list below includes the first sentence of each security measure. The summary is intended to improve understanding of the security measures and is not a substitute for the formal definition of the security measures for EO-critical software use in the previous table, which contains additional details for some security measures and provides informative references for all security measures.

Objective 1: Protect EO-critical software and EO-critical software platforms from unauthorized access and usage.

- **SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators** of EO-critical software and EO-critical software platforms. (See FAQ #7.)
- **SM 1.2: Uniquely identify and authenticate each service** attempting to access EO-critical software or EO-critical software platforms.
- **SM 1.3: Follow privileged access management principles for network-based administration** of EO-critical software and EO-critical software platforms.
- **SM 1.4: Employ boundary protection techniques as appropriate** to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.

Objective 2: Protect the confidentiality, integrity, and availability of data used by EO-critical software and EO-critical software platforms.

- **SM 2.1: Establish and maintain a data inventory** for EO-critical software and EO-critical software platforms.
- **SM 2.2: Use fine-grained access control for data and resources** used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.
- **SM 2.3: Protect data at rest** by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.
- **SM 2.4: Protect data in transit** by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.
- **SM 2.5: Back up data, exercise backup restoration, and be prepared to recover data** used by EO-critical software and EO-critical software platforms at any time from backups.

Objective 3: Identify and maintain EO-critical software platforms and the software deployed to those platforms to protect the EO-critical software from exploitation.

- **SM 3.1: Establish and maintain a software inventory** for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.
- **SM 3.2: Use patch management practices** to maintain EO-critical software platforms and all software deployed to those platforms.
- **SM 3.3: Use configuration management practices** to maintain EO-critical software platforms and all software deployed to those platforms.

Objective 4: Quickly detect, respond to, and recover from threats and incidents involving EO-critical software and EO-critical software platforms.

- **SM 4.1: Configure logging to record the necessary information about security events** involving EO-critical software platforms and all software running on those platforms.
- **SM 4.2: Continuously monitor the security** of EO-critical software platforms and all software running on those platforms.
- **SM 4.3: Employ endpoint security protection** on EO-critical software platforms to protect the platforms and all software running on them.
- **SM 4.4: Employ network security protection** to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.
- **SM 4.5: Train all security operations personnel and incident response team members, based on their roles and responsibilities,** on how to handle incidents involving EO-critical software or EO-critical software platforms.

Objective 5: Strengthen the understanding and performance of humans' actions that foster the security of EO-critical software and EO-critical software platforms.

- **SM 5.1: Train all users of EO-critical software, based on their roles and responsibilities,** on how to securely use the software and the EO-critical software platforms.
- **SM 5.2: Train all administrators of EO-critical software and EO-critical software platforms, based on their roles and responsibilities,** on how to securely administer the software and/or platforms.
- **SM 5.3: Conduct frequent awareness activities** to reinforce the training for all users and administrators of EO-critical software and platforms, and to measure the training's effectiveness for continuous improvement purposes.