Security Measures for "EO-Critical Software" Use

Karen Scarfone

karen.scarfone@nist.gov

Guidance development process

EO 14028, 4(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****.*

- Determined the purpose and scope of the guidance
- Reviewed and provided feedback on draft definitions of "EO-critical software"
- Defined objectives for the security measures to meet
- Identified and prioritized possible security measures for inclusion
- Drafted the guidance and revised it based on reviewer feedback

- Received nearly 90 position papers from the community addressing critical software use security measures
- Hosted a virtual workshop to gather additional input
- Consulted with CISA and OMB on security measures

Guidance development

Motivation

- Even though EO-critical software may be developed using recommended secure development practices, it still needs to be secured in agencies' operational environments.

Purpose and scope

- Protect the use of agencies' deployed EO-critical software
- Development and acquisition of EO-critical software are out of scope

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.

Objectives for 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.
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.

Security measure example

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

Objective 1 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.
	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 security measures

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 security measures

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 security measures

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 security measures

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.