Executive Order 14028 on Improving the Nation's Cybersecurity: 3 Years in, Where Are We?

Katell Thielemann

Gartner®

Key Issues

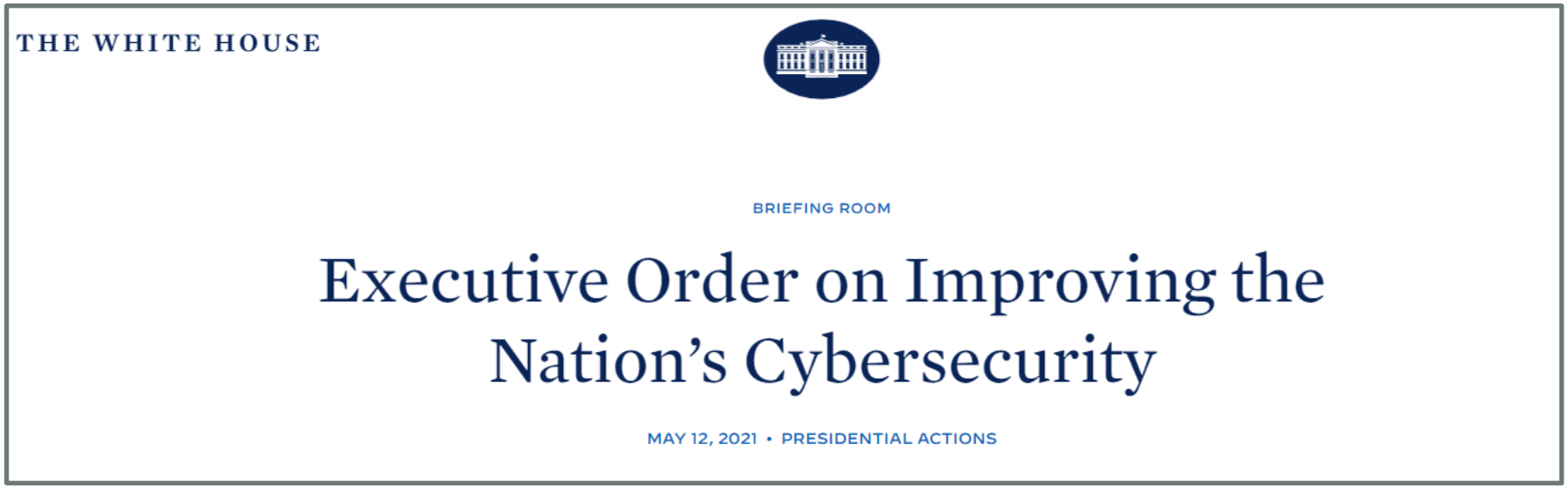
1. Progress report.
2. Implications for agencies and federal vendors.
3. Gaps and the way forward.

Gartner®

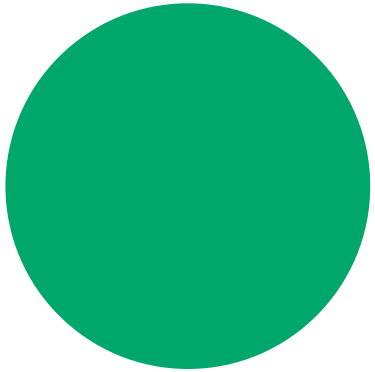
Key Issues

1. Progress report.
2. Implications for agencies and federal vendors.
3. Gaps and the way forward.

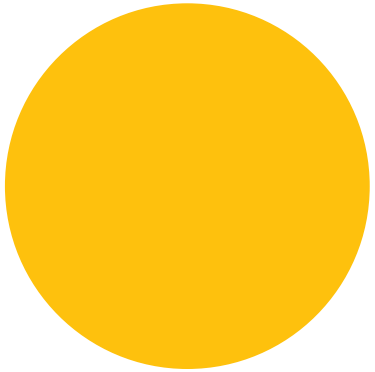
Gartner®



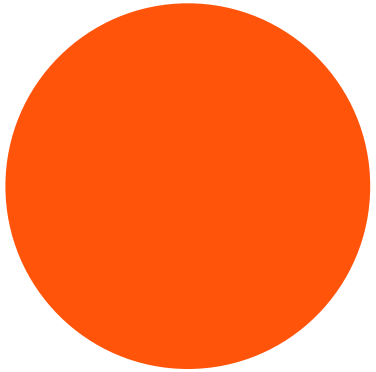
- Section 1: Policy
- Section 2: Removing Barriers to Sharing Threat Information
- Section 3: Modernizing Federal Government's Cybersecurity
- Section 4: Enhancing Software Supply Chain Security
- Section 5: Establishing a Cyber Safety Review Board
- Section 6: Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
- Section 7: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks
- Section 8: Improving the Federal Government's Investigative and Remediation Capabilities
- Section 9: National Security Systems



Implemented



In progress with positive momentum



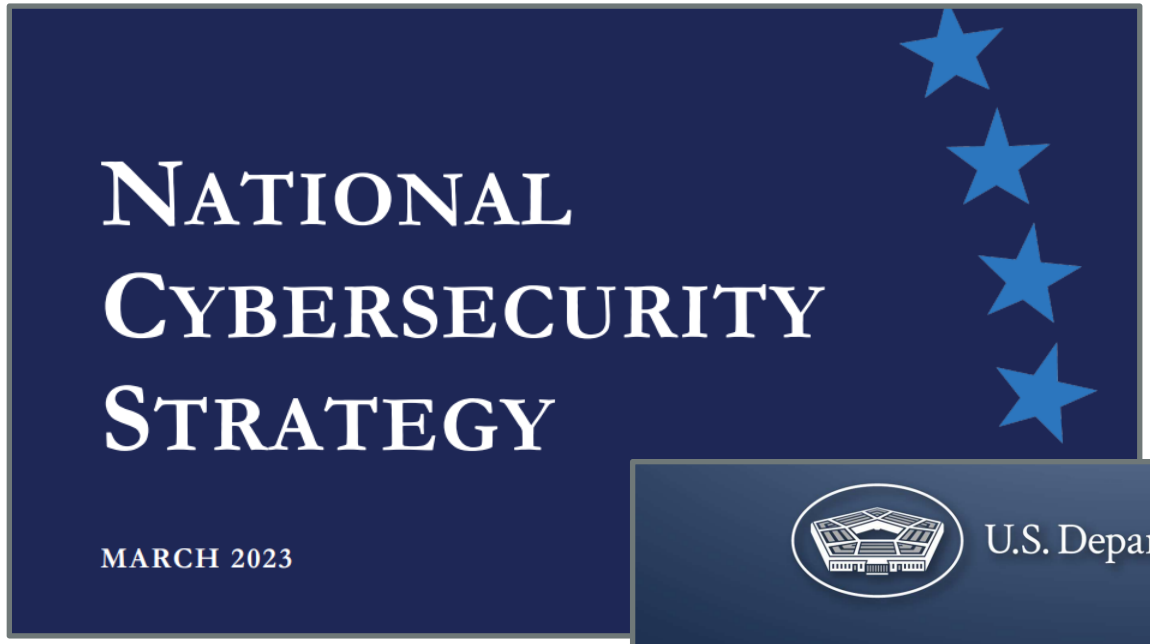
In progress with many difficulties

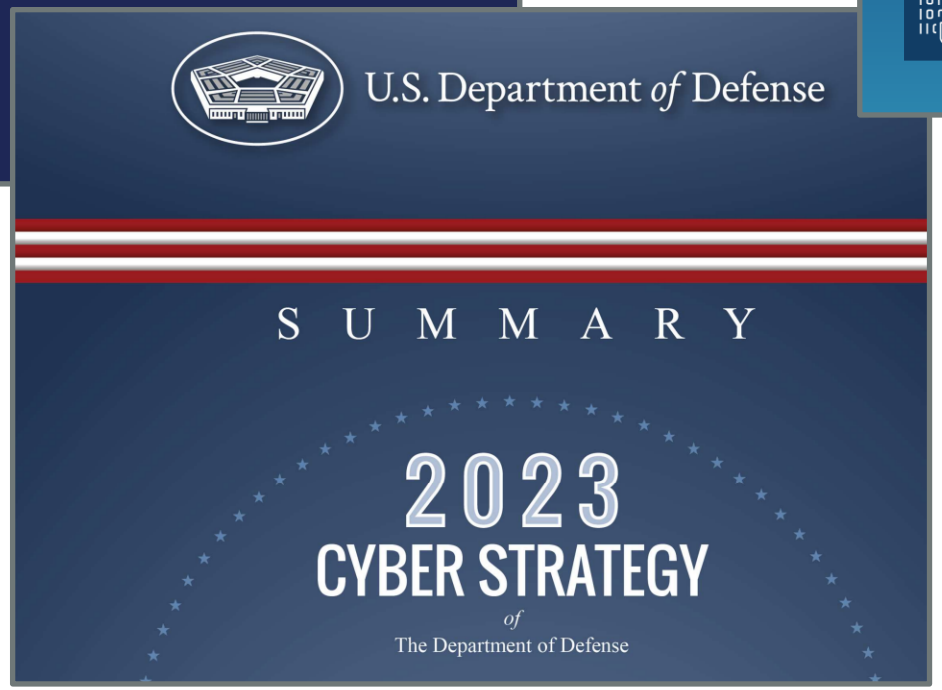
Gartner®

Section 1: Policy (2021)

- The U.S. faces **persistent** and **increasingly sophisticated** malicious cyber campaigns that threaten the public sector, the private sector, and ultimately, the American people's security and privacy …
- The federal government must improve its efforts to **identify, deter, protect against, detect and respond …**
- The **private sector** must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the federal government to foster a more secure cyberspace …
- The federal government needs to make **bold changes** and **significant investments …**
- The scope … must include systems that process data (IT) and those that run the vital machinery that ensures our safety (operational technology [OT]) — aka cyber-physical systems.
- It is the policy of my administration that the prevention, detection, assessment and remediation of cyber incidents is a **top priority and essential to national and economic security.**

2024





Gartner®

Section 2: Removing Barriers to Sharing Threat Information

Focus of EO 14028

- Remove contractual barriers; streamline security mandates for contractors.
- Manage information reported by agency-contracted vendors.
- Require IT service providers to share breach information that could impact government networks — extend DFARS 252.204.7012 clause to all contractors.
- Develop procedures for interagency sharing.

Progress update

- Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA); CISA working on implementation.
- Proposed new Federal Acquisition Regulations (FAR) rule:
  - — Revise the definition of “ICT” to include cyber-physical systems (OT/ICS).
  - — Reporting requirement to CISA within eight hours.
  - — Grants CISA, the FBI and the contracting agency “full access” to systems and personnel.
- DHS report on duplicative federal cybersecurity incident reporting requirements (September 2023).
- NSM-22: intel agencies must share more.

DFARS = Defense Federal Acquisition Regulation Supplement; CISA = Cybersecurity and Infrastructure Security Agency; ICT = information and communication technology; NSM = National Security Memorandum; DHS = Department of Homeland Security

Gartner®

Section 3: Modernizing Federal Government's Cybersecurity

Focus of EO 14028

- Agencies to move toward zero-trust principles and initially focus on some specific tools.
- Agencies to evaluate the types and sensitivity of unclassified data they use and provide a report to CISA and OMB.
- CISA to release cloud security technical reference architecture document.
- Agencies to amplify the use of multifactor authentication and encryption for data at rest and in transit.
- Agencies to update the existing plans to prioritize resources for the adoption and use of cloud technology.

Progress update

- CISA updated the zero-trust maturity model.
- OMB M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.

  — CISA guidance around logging requirements (February 2023).
- M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

  — Mandated actions for agencies around identity, devices, networks, applications and workloads, and data.
- DoD v.5.0 of its Cybersecurity Reference Architecture (CSRA).

OMB = Office of Management and Budget

Gartner

Section 4: Enhancing Software Supply Chain Security

Focus of EO 14028

- Improve the security of software by establishing baseline security standards for the development of software sold to the government.

Progress update

- NIST critical software definition.
- NTIA guidance on minimum SBOM elements.
- M-21-30: Protecting Critical Software Through Enhanced Security Measures.
- M-22-18: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.
  - — Attestations and SBOMs; FAR council new part 40.
  - — M-23-16: Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.
- CISA/NSA/ODNI developers, suppliers and consumers guides (8 November 2022).
- GSA letter MV-23-02: Ensuring Only Approved Software Is Acquired and Used at GSA (February 2023).
- March 2024: CISA, OMB release secure software development attestation form — **8 June** CISA RSAA portal.

NSIT = National Institute of Science and Technology; NTIA = National Telecommunications and Information Administration; SBOM = software bill of materials; NSA = National Security Agency; ODNI = Office of the Director of National Intelligence; GSA = General Services Administration; RSAA = Repository for Software Attestations and Artifacts

Gartner®

Section 4: Enhancing Software Supply Chain Security

Focus of EO 14028

- Create consumer Internet of Things (IoT) labeling — akin to “ENERGY STAR.”
- Set the stage for other activities.

Progress update

- Various NIST documents + Federal Communications Commission (FCC) published a notice of proposed rulemaking regarding the creation of a voluntary “Cyber Trust Mark” cybersecurity labeling program for IoT devices (August 2023).

- CISA released “HBOM Framework for Supply Chain Risk Management” (09/2023).
- CISA published the Open-Source Software Security Roadmap (September 2023).
- “Secure by Design” pledge by 68 companies at the RSA2024 conference.

Section 5: Establishing a Cyber Safety Review Board

Focus of EO 14028

- Modeled after National Transportation Safety Board.

Progress update

- Established 3 February 2022; high-profile members.
- Initial focus: Apache Log4j; report (July 2022).
- Report on Lapsus$ and related threat groups (August 2023).
- Report on Microsoft Online Exchange Incident from Summer 2023 (April 2024).
- New leaders added to the board (May 2024).
- Congress evaluating tweaks to increase independence and transparency.

Section 6: The Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents

Focus of EO 14028

- Standard set of operating procedures (playbook) and a set of definitions for cyber incident response by federal departments and agencies.

Progress update

- DHS binding operational directive (BOD) on vulnerabilities.
- CISA-known exploited vulnerabilities catalog released.
- CISA incident and vulnerability response playbooks; OMB guidance on how to use.
- M-23-03: Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements.
  - — Updates to incident reporting and handling processes.
- M-24-04: Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements.
  - — Doubles down.

Section 7: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks

Focus of EO 14028

- Governmentwide endpoint detection and response system.
- Agencies must establish or update memorandums of agreement (MOAs) with CISA for the Continuous Diagnostics and Mitigation Program.

Progress update

- M-22-01: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems Through Endpoint Detection and Response.
- CISA BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks.

- GAO 12/2023: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements.
- CISA “vulnrichment” program (May 2024).

Section 8: Improving the Federal Government's Investigative and Remediation Capabilities

Focus of EO 14028

- Cybersecurity event log requirements for federal departments and agencies.

Progress update

- M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident.
  - — Focus on logging, visibility to the enterprise SOC*.
- GAO report shows low agency maturity against logging requirements.
- CISA worked with Microsoft to offer free logging capabilities to agencies (February 2024).

SOC = security operations center

Gartner

Section 9: National Security Systems

Focus of EO 14028

- Originally largely out of scope.

Progress update

- National Security Memorandum/NSM-8 on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (January 2022).

  — EO applies to NSS — cloud adoption, MFA*, encryption, zero trust and others.

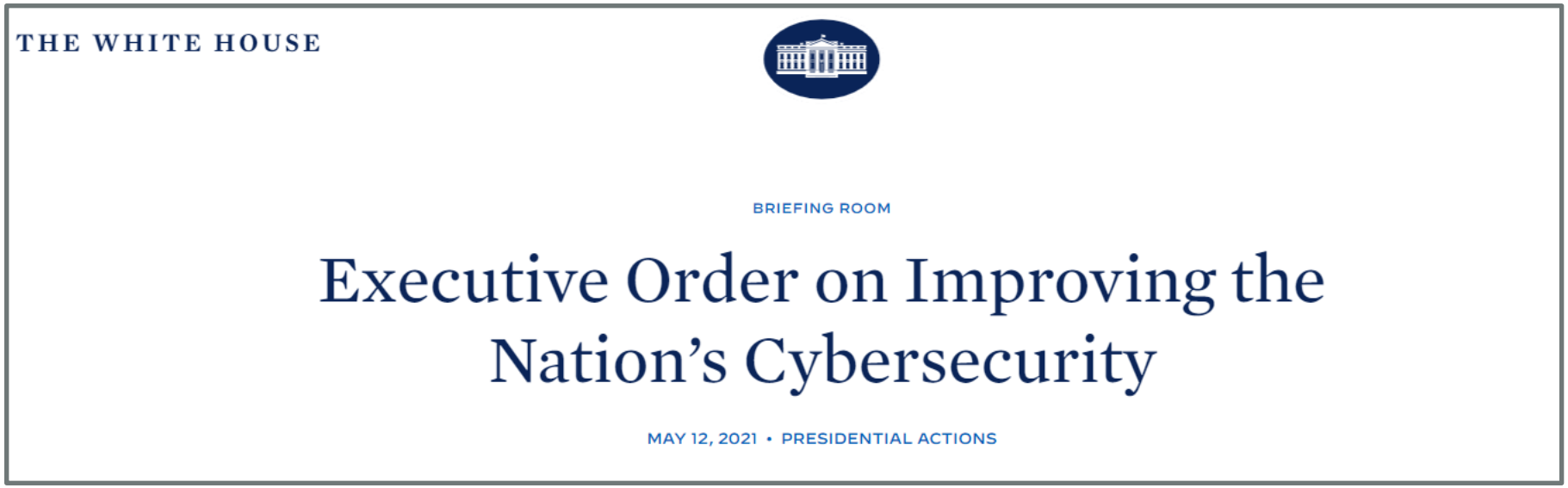
  — New guidance on minimum security standards for national security systems in the cloud.

  — NSA binding operational directive authority.

  — DHS and NSA to collaborate on the development of emergency directives and binding operational directives for agencies.
- DoD zero-trust strategy.

MFA = multifactor authentication

Gartner



- Sec. 1: Policy
- Sec. 2: Removing Barriers to Sharing Threat Information
- Sec. 3: Modernizing Federal Government's Cybersecurity
- Sec. 4: Enhancing Software Supply Chain Security
- Sec. 5: Establishing a Cyber Safety Review Board
- Sec. 6: Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
- Sec. 7: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks
- Sec. 8: Improving the Federal Government's Investigative and Remediation Capabilities
- Sec. 9: National Security Systems

Key Issues

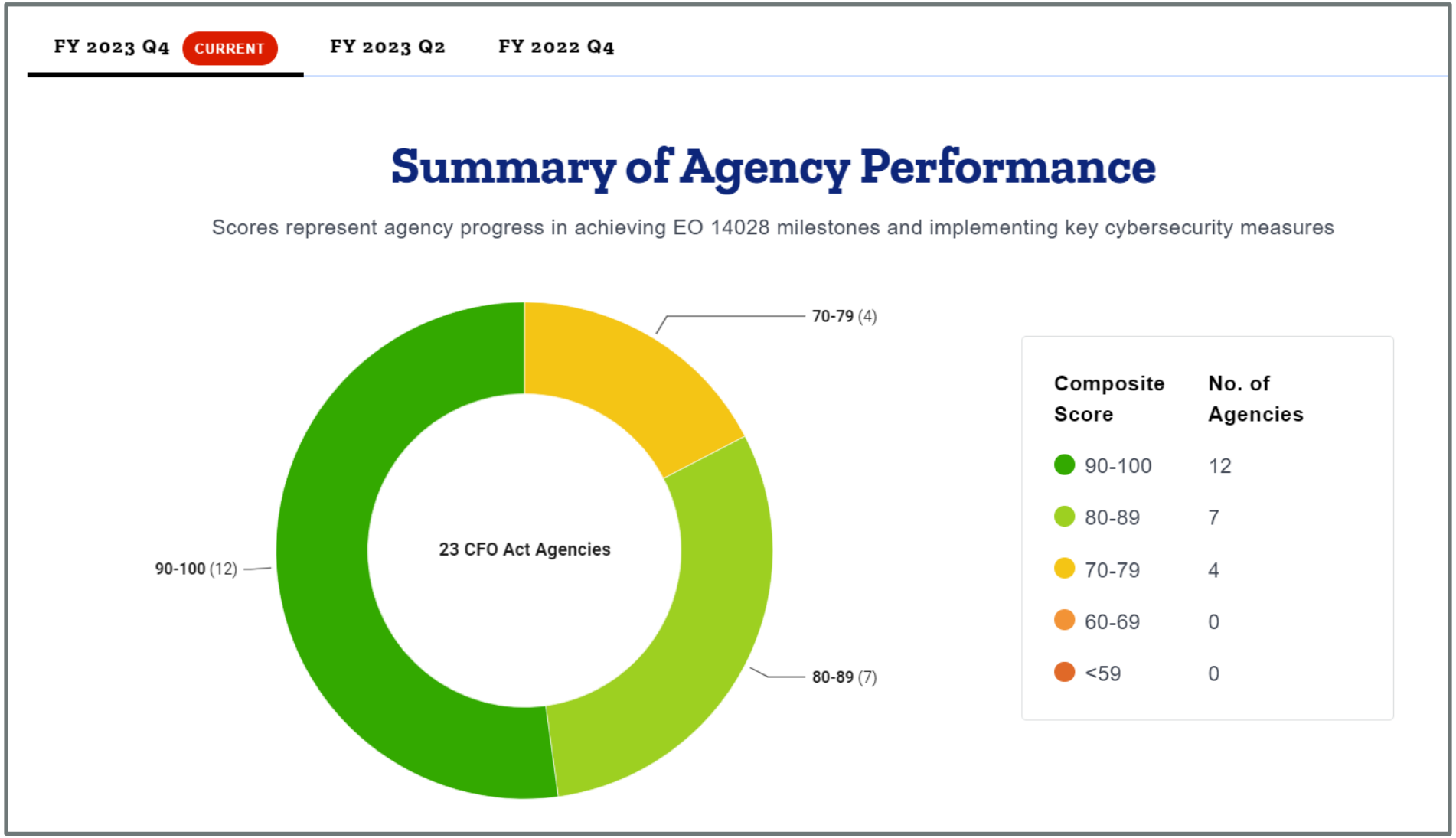
1. Progress report.
2. Implications for agencies and federal vendors.
3. Gaps and the way forward.

Implications for Agencies

- Over 55 actions in the EO; hundreds more in OMB memos, CISA binding directives and new strategies.
- Aggressive timelines.
- No immediate budget added; budget cycles disconnected.
- FISMA metrics updated.
- Participate in the FAR changes process, then implement.
- Large-scale internal employee communications and training (e.g., MFA).
- Existing contracts will likely need to be amended (e.g., phishing-resistant MFA is mandatory for contractors as well).

Gartner®

Performance.gov



Source: Federal Cybersecurity Progress Report, Performance.gov

Gartner

Implications for Federal Vendors

- Important FAR changes.
- More mandates/cost/confusion:
  - — In addition to CMMC, FedRAMP and C2M2.
- More “reach in” in case of incidents.
- More oversight — False Claims Act actions?
- Opportunities to sell more security solutions and services:
  - — “Zero trust” marketing blitz.

CMMC = Cybersecurity Maturity Model Certification; FedRAMP = Federal Risk and Authorization Management Program; C2M2 = Cybersecurity Capability Maturity Model

Gartner®

Key Issues

1. Progress report.
2. Implications for agencies and federal vendors.
3. Gaps and the way forward.

Gaps — What's Missing So Far?

- Formally structured updates:
  - — Updates fly in from GAO, CRS, NIST, CISA, OMB, DoD, …
- Evidence that all these activities improve security.
- Specificity around "IoT" and "OT" systems, which are CPS with unique security considerations:
  - — Sectorial sprints and directives.
  - — NIST SP 1800-10, "Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector."
- FAR contractual changes — formal rulemaking is hard …
- CISA-issued list of critical software.

GAO = Government Accountability Office; CRS = Congressional Research Service
Source: Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector, NIST

The Way Forward

- Need for ONCD cyber regulations harmonization (e.g., incident reporting).
- Need for Congress to legislate on what works — EOs can come and go.
- Need to see how/if secure software attestation forms process work.
- Need to streamline nomenclature:

  — For example: 2024 NDAA calls out “operational technologies,” while OMB Memo M-24-04, calls out IoT “the interconnected devices that interact with the physical world — from building maintenance systems, to environmental sensors, to specialized equipment in hospitals and laboratories,” and NIST SP 1900-202 documents the equivalency of IoT and CPS. Gartner covers the security of OT/IoT/IIoT/IoMT under the CPS umbrella.

- More focus on shared services.

ONCD = Office of the National Cyber Director; IIoT = Industrial Internet of Things; IoMT = Internet of Medical Things; NDAA = National Defense Authorization Act

Gartner®

But Wait! There's More!

EO 14028 — May 2021 — various sections call out

New! **Inaugural Report on the Cybersecurity Posture of the United States — May 2024 —** Congress-mandated report form ONCD

CIRCIA — March 2022 — incident reporting bill signed into law
CIRCIA — June 2024 — extended deadline for public comments New!

New! **National Cybersecurity Implementation Plan v.2 — May 2024 —** update on prior efforts and adds 31 actions

Updated National Cybersecurity Strategy — March 2023 — builds upon but pushes much further than prior strategies

New! **National Security Memorandum on Critical Infrastructure Security and Resilience — April 2024 —** replacement of PPD-21 from 2013

National Cybersecurity Implementation Plan v.1 — July 2023 — 69 actions

President Council of Advisors on Science and Technology Report — February 2024 focus on the need for cyber-physical resilience New!

Gartner®

Recommendations

- Federal agencies:
  - Prioritize budget requests to align to mandates.
  - Weigh the pros and cons of shared services.
- Vendors:
  - Closely track new mandates that will affect you.
  - Deliberately map your security offering to agency actions.
- All:
  - Join government-industry groups.
  - Engage in the harmonization discussion.

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- **Predicts 2024: U.S. Federal Government**
  Michael Brown and Daniel Snyder
- **Mitigate Enterprise Software Supply Chain Security Risks**
  Dale Gardner
- **Use the U.S. DoD Model for Your Zero Trust Approach: Network & Environment Pillar**
  Thomas Lintemuth
- **Innovation Insight for SBOMs**
  Manjunath Bhat, Dale Gardner and Mark Horvath
- **Infographic: 2024 Planned Technology Spend for CIOs in U.S. Federal Government and Defense**
  Michael McFerron, Michael Brown and Dean Lacheca

Access to Gartner research is subject to individual subscription type and product entitlements.

Gartner®