Operational Technology Cybersecurity Coalition

Sector Risk Management Agency Maturity Model

Abstract

Recent cyberattacks on critical infrastructure have underscored a persistent challenge: the inconsistent cybersecurity maturity across the federal government's Sector Risk Management Agencies (SRMAs). To address this critical national security gap, this document proposes a new framework for the Office of the National Cyber Director (ONCD) to evaluate and improve the cybersecurity capabilities of these agencies. The model would enable ONCD to annually evaluate SRMAs on a 1-to-5 scale based on their domain expertise, policies, risk assessments, incident response, and cross-sector coordination—especially in operational technology (OT) environments. The framework is designed to align with existing mandates and standards, while establishing consistent benchmarks for federal budgeting, sector-specific performance metrics, and collaboration with industry. The overarching goal is to enhance national critical infrastructure resilience by identifying SRMA gaps, guiding investment, and enabling both public and private sectors to plan for continuous cybersecurity improvement.

About the OTCC

The Operational Technology Cybersecurity Coalition is a diverse group of leading cybersecurity vendors representing the entire OT lifecycle. The OT Cyber Coalition believes that the strongest, most effective approach to securing our nation's critical infrastructure is one that is open, vendor-neutral, and allows for diverse solutions and information sharing without compromising cybersecurity defenses.

Authors

Tatyana Bolton
Executive Director
Operational Technology Cybersecurity Coalition (OTCC)

Mark Montgomery
Center on Cyber and Technology Innovation Senior Director and Senior Fellow
Foundation for Defense of Democracies (FDD)

Introduction

As the type, severity, and volume of cybersecurity attacks against critical infrastructure grow, it's becoming increasingly important for policymakers in the public and private sectors to better assess the preparedness and capabilities of our national critical infrastructure to quickly recover from a cyberattack. Essential to that understanding is an established mechanism for how we should measure cybersecurity capabilities within each SRMA. As a country, when using such a mechanism, we should also understand how much we want to budget for that cybersecurity protection, and what level of cybersecurity preparedness we expect. By having an agreed-upon set of capabilities that must be present across public and private sectors, federal officials and their private sector partners would be better able to determine the level of federal investment necessary for achieving the desired state of preparedness.

In order to implement these ideas, ONCD in coordination with the Cybersecurity and Infrastructure Security Agency (CISA) should begin to annually grade the maturity of each SRMA. This framework will measure functional capabilities, and account for OT-specific challenges, especially in sectors heavily reliant on legacy systems and real-time operations. By establishing this framework, ONCD, in coordination with the Office of Management and Budget (OMB), could more effectively fulfill its mandate by shaping federal cybersecurity budgets and tracking SRMA maturity over time. ONCD and OMB would then also be able to provide better budget guidance to meet expectations as set forth in the National Cybersecurity Strategy.

The maturity scale includes criteria that assess a SRMA's ability to provide recommendations, integrate OT-specific cybersecurity standards (e.g., NIST SP 800-82, IEC 62443) into incident response and risk management plans, propose sector-specific best practices, and measure overall preparedness for real-time monitoring and incident response. By taking these steps, agencies can more effectively collaborate with the private sector to secure the sector's IT and OT environments and systems. This framework would also serve as a basis for targeted initiatives aimed at deepening sector-specific expertise.

Criteria for assessment will be organized into the following categories:

- Domain Expertise
- Policy
- Risk Assessment
- Incident Response
- Cross-Sector Coordination

The categories are based on the roles and responsibilities SRMAs are mandated to carry out, as outlined in ONCD's National Security Memorandum 22 (NSM-22). As a reminder, those responsibilities include: coordinating sector-specific activities; providing technical expertise and assistance; serving as the Federal Government coordinating council chair; participating in cross-sector coordinating councils; conducting sector-specific risk assessments; identifying essential workforce needs for the sector; and identifying sector-specific information and facilitating information sharing; among others. As that framework evolves, this model can also evolve to match new structures but must exist to bolster our resilience.

SRMAs should use the NIST Cybersecurity Framework (CSF) and the International Electrotechnical Commission (IEC) 62443 as starting points, and supplement sector-specific guidance. The SRMA should provide performance metrics for achieving advanced levels of maturity, as opposed to leaving those metrics up to each individual organization. SRMAs should also expand on CSF's guidance to include Software Bill of Materials (SBOMs) as common critical components, identify minimal viable service objectives, and create a trusted registry of suppliers to support supply chain security. This maturity model would allow SRMAs to identify resilience requirements and provide assessment metrics. It will also allow policymakers at the state and federal levels, as well as industry, to come up with coordinated plans for improvement.

Below is a framework that turns SRMA roles and responsibilities categories into actionable and measurable criteria, enabling policymakers to identify the maturity of the SRMA and provide a roadmap (and the necessary investment levels) for improvement. The private and public sectors will jointly develop this roadmap.

In terms of SRMA maturity, ONCD should rate each SRMA on a scale of 1 to 5, 1 being inconsistent maturity, 5 being optimized maturity. To reach a designated level of maturity, the SRMA must meet 70 percent of the requirements in that particular ranking for rankings 2-3. For 4 and 5, all metrics must be met. For those organizations who are a level 1 or 2 maturity, ONCD should require a yearly report outlining a plan for improvement to be provided by the SRMA to the ONCD.

Sector Risk Management Agency Categories of Maturity

1

Inconsistent Maturity

Domain Expertise:	Possesses limited cybersecurity domain expertise.
Policies:	Security policies are outdated (older than 5 years old).
Risk Assessment:	Does not pursue any risk assessment.
Incident Response:	Does not have incident response plans.
Cross-Sector Coordination:	Does not have any cross-sector coordination or information sharing.

2

Basic Maturity

Domain Expertise:	Presence of initial domain expertise within the SRMA, meaning the SRMA is working to understand what cybersecurity needs are both important and unique to the sector. The SRMA is working to achieve visibility into what resources and tools are being used, and identifying essential workforce needs for the sector.
Policies:	Working to develop basic security policies such as: ◦ Risk Management Framework ◦ Access Control Policies ◦ Vulnerability Management Policy ◦ Incident Response Plan Policies are drafted but may lack regular updates.
Risk Assessment:	Working to establish basic sector risk assessment processes.
Incident Response:	Basic incident response plans exist but may lack testing, coordination, or clear responsibilities. Existence of a published sector incident response plan, but lacks sufficient training and annual reinforcement.
Cross-Sector Coordination:	Nascent information sharing efforts without consistent and coordinated processes. Limited or no Information Sharing and Analysis Center (ISAC) process.

3 Structured Maturity (All Items for 2 Above, Plus)

Policies: The SRMA has an overview of the entities within the sector. Well-documented and updated guidance, such as how to conduct good risk management, aligned with industry best practices.

Risk Assessment: Regular sector risk assessments are performed, and risk management strategies are updated for critical entities and systems.

Incident Response: Annual tabletop exercise with CISA and the FBI to test the agency response plan. Annual tabletop exercise with sector partners to test the sector response plan. Annual cross sector tabletop exercise with sector partners as well as agencies/sectors that represent significant interdependencies.

Cross-Sector Coordination: Detailees from agency to CISA watch floor, and from CISA to agency, to build relationships and understanding of roles/responsibilities of agency and CISA. SRMA conducts regular marketing efforts to drive adoption of CISA's free cyber hygiene tools. The sector managed by the SRMA effectively uses CISA's free cyber tools as needed.

4 Managed Maturity (All Items for 2 and 3 Above, Plus)

Policies: Security policies and procedures are regularly reviewed, updated, and effectively communicated across the sector. The SRMA has Cyber Performance Goals for its sector and manages those with sector partners.

Risk Assessment: Regular sector risk assessments are performed, and risk management strategies are updated for all entities and systems. The SRMA must conduct an annual "census" of their industry to assure that the SRMA engages the sector at a statistically significant level.

Incident Response: Where applicable, well-established incident response capabilities, continuous monitoring, and regular drills or simulations.

Cross-Sector Coordination: Clear and delineated roles and responsibilities between SRMAs, ISACs, and Sector Coordinating Councils (SCCs). 70 percent of the sector participates in industry's ISAC and SCC.

5 Optimized Maturity (All Items for 2, 3 and 4 Above, Plus)

Risk Assessment: For each National Critical Function, the SRMA must work with CISA, the sector, and their Sector Coordinating Councils to identify minimum viable delivery objectives for services.

Incident Response: The SRMA must produce an annual report to the DHS CISA National Risk Management Center and the ONCD that:

- Describes the sector's resistance and preventative measures to disruptive cyberattacks. Efforts should include isolating and recovering OT systems; strategies for maintaining operational continuity during cyberattacks; and information sharing with relevant sector partners and stakeholders.
- Lists the number of significant cyber incidents in the sector over the last year.
- Describes the severity of each cyber incident that took place over the last year.

Cross-Sector Coordination: The SRMA can map and measure interdependencies that its sector has with other critical infrastructure sectors. Shows consistent improvement and strives to advance security across ecosystem partners and other sectors.

Additional Information

For SRMAs that are rated as a 1 by ONCD, CISA must provide:

- A generic agency incident response plan, that the agency will use in the event of an incident
- A sector risk management response plan, that the agency will use in the event of an incident
- Generic cybersecurity expertise will be made available to the SRMA and that expertise will manage the agency's government coordinating council and serve as the SRMA's representative to the SCC

Appendix:

Risk Assessment:

Each sector should be able to identify the critical entities and infrastructure within its sector in order to develop complete risk assessments tailored to effectively address OT-specific threats and vulnerabilities. SRMAs rated at level 3 or higher should be mandated to conduct comprehensive risk assessments that specifically evaluate OT risks, such as unpatched legacy systems, supply chain vulnerabilities, and the potential physical impact of cyber incidents. Further, cross-sector interdependencies should be included in risk assessments for SRMAs rated at levels 3 and above.

Incident Response:

SRMAs are required to develop incident response plans under NSM-22. In addition to developing an incident response plan, it is critical to make timely updates to reflect the ever-evolving threat landscape within the sector.

For SRMAs in sectors with significant amounts of OT, response plans must incorporate both IT and OT. OT incidents involve unique safety and operational concerns that may not align with IT-centric incident response plans. Further, simulating OT cyber incidents ensures that SRMAs and their sector partners are adequately prepared. This includes collaborating with OT security experts to ensure that responses do not inadvertently disrupt critical operational processes, as well as working across sectors that pose interdependent risk. Annual tabletop exercises required for SRMAs rated at levels 3 and above should include OT-specific drills that simulate potential cyber incidents affecting OT systems.

Cross-Sector Coordination and Information Sharing:

Given the interconnectedness of OT systems across sectors like energy, transportation, and manufacturing, SRMAs managing OT environments should prioritize cross-sector coordination and information sharing for managing systemic risk. For SRMAs rated at levels 4 and 5, regular participation in OT-specific ISACs and cross-sector OT security coordination efforts should be required. This will enhance both sector-specific and cross-sector threat intelligence sharing, particularly focusing on OT vulnerabilities and attack vectors.

Cyberattacks and Resilience:

Cyberattacks pose a distinct risk to OT systems that control physical processes. SRMAs should be evaluated on their ability to handle cyber incidents targeting OT systems. Given the potential physical impact of a cyberattack on OT environments, SRMAs rated at level 5 should develop OT-specific resilience plans. These plans should include steps for isolating and recovering OT systems without disrupting essential services, strategies for maintaining operational continuity during ransomware attacks, and information sharing with relevant stakeholders across the sector, necessary departments, and agencies.