Cyber Supply Chain Risk Management Implementation Procedures & Guidelines

February 27, 2024

U.S. Office of Personnel Management

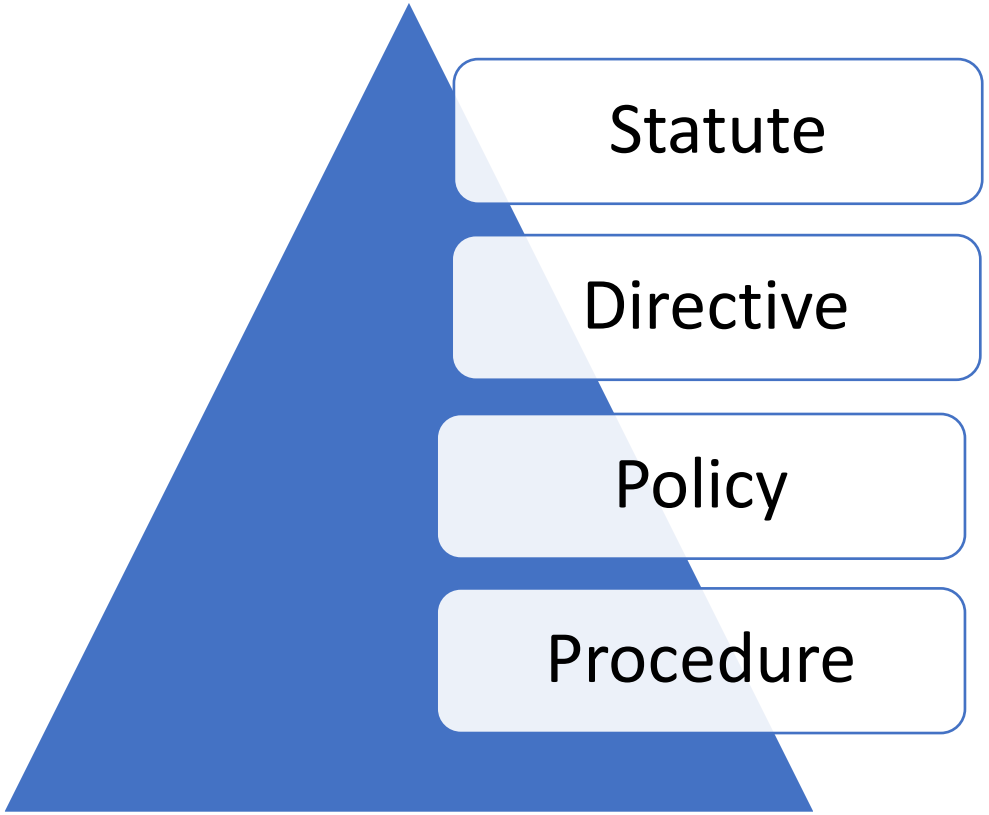
Agenda

- OPM Cybersecurity Program
- High-Level C-SCRM Strategy
- Selected NIST Controls
- Open Forum

OPM Cybersecurity Program

U.S. Office of Personnel Management

Structural Hierarchy



FISMA 2014, Privacy Act of 1974, Supply CHAIN Act of 2021

OMB A-130, OMB A-108, OMB Federal Acquisition Supply Chain Security Act

OPM Cybersecurity and Privacy Policy

Procedures, Guidelines, Guidance, SOPs, Baselines, Standards

You are here.

Policy Versus Procedure

- One of the key differences between policy and procedure is “how.” Once you start telling people how, you’re beyond policy.
- The original request from the Forum was a Standard Operating Procedure or SOP.
- OPM publishes a set of Implementation Procedures and Guidelines for each NIST SP 800-53-5 control family as well as several other things.
- The term “implementation procedures and guidelines” itself is a rather transparent effort to be a catch-all of sorts; to provide direction that is procedural in nature and to the level of detail necessary, for the individual control. This includes implementation strategy.
- These documents also provide caveats, scoping guidance, and practical limitations for the implementation of each control.

A Parallel Example: RA-05 (05)

5.5 VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS [RA-05 (05)] [M, H]

All IT systems and services must undergo vulnerability scanning for all components (physical and virtual, production and non-production environments) using local admin or root equivalent privileges on a weekly basis. The account used to scan should be managed as a 'service account' and must be configured to not allow interactive login.

Authenticated vulnerability scanning with privileged access must be conducted when possible. Some devices may be provided to the organization as an appliance, where no method for operating system level authentication is possible, or where doing so violates the manufacturer warranty or service agreement. In these cases, unauthenticated scanning may be the only available option.

High-Level C-SCRM Strategy

Our Strategy? Be Pragmatic

- The first step in OPM's C-SCRM Strategy is to understand OPM's role.
- OPM is not part of the intelligence community. Although OPM does have a Cyber Threat Intelligence (CTI) capability, OPM cannot conduct counter-intelligence investigations on persons or companies.
- OPM's role is associated with due diligence regarding C-SCRM. OPM can and does conduct due diligence C-SCRM practices like any commercial consumer.
- OPM's C-SCRM plan focuses on due diligence throughout the five functional areas of the NIST CSF both prior to and after utilizing a particular company (provider) and product (component). The frequency or rigor of the due diligence activity varies, where due diligence activities related to detection and response occur more regularly than pre-acquisition due diligence activities.

The Types of IT We Buy

- OPM's C-SCRM Strategy starts with the acquisition process.

- The agency's IT-related purchases generally fall into the following categories:
  - Hardware (e.g., laptops, servers, routers, and peripherals),
  - COTS software,
  - Custom software supported by contract,
  - Open-Source Software, and
  - Services (typically cloud-based).

Not All Controls Are Created Equal

- Using NIST SP 800-53-5 and 800-53B baselines as a starting point, we sought to understand what we're doing now, and if nothing, what we should be realistically doing, for each control.

- We also looked closely at which controls provided bona fide value to our C-SCRM program, versus which ones were less so. These latter group of controls could be earmarked for future tailoring-out.

- Agencies are allowed to tailor the NIST SP 800-53B baseline selections, provided that they've conducted some type of risk-based justification that leadership has approved.

[overheard by a senior official at a cabinet-level agency]

"Don't we have a team that looks for these things; that opens up laptops and looks for counterfeit microchips and stuff?"

"No, no we do not."

[if we were to do that]

A) We'd likely void the manufacturer warranty that we rely on.

2) We'd likely catch only very sloppy criminals, if that.

d) We'd likely cause more harm than good (refer to item A).

Selected NIST Controls

Supply Chain Risk Management Plan | Establish SCRM Team [SR-02 (01)]

Remember that not all risk management and not all supply chain risk management happens in Cyber or even within an Office of the CIO.

It is strongly recommended that you establish and sustain an open and collaborative relationship with your agency's Enterprise Risk Management (ERM) Board or equivalent – at OPM we call it the Risk management Council (RMC).

Talk to them. Ask them what they want to know more about. Ask them what their concerns are. Brief them regularly on these things. About the mechanisms your team has in-place. About the limitations those mechanisms have.

One of the biggest risks for your CISO is your leadership team thinking that you have a capability to respond to a C-SCRM problem that you do not in fact have. After the problem occurs is probably not the time to break the news to them.

C-SCRM Starts with Acquisition

- Supply Chain Controls and Processes [SR-03]
- Acquisition Strategies, Tools, and Methods [SR-05]

These controls are very closely related and all point back to the same thing: You need to have a very open and cooperative relationship with your Procurement Operations team and Senior Procurement Executive (SPE). Otherwise, your C-SCRM program will not be effective.

Let's be honest: this was true before C-SCRM became the new hot topic.

Per FITARA, the CIO should be approving all IT buys, which means Cyber should be reviewing all IT buys. If your SOWs, SOOs, and PWSs do not have the necessary requirements in them to compel your contracts to get you the visibility you need (e.g., scanning, SIEM, EDR, incident notification), then you will be at a significant disadvantage until that changes.

Supplier Assessments and Reviews [SR-06]

At a foundational level, this should already be happening:

- The CO should be documenting that the awardee meets FAR part 9.104-1 (standards of responsibility for contractors) prior to award.
- There's also the Contractor Performance Assessment Reporting System (CPARS) the Federal Awardee Performance and Integrity Information System (FAPIIS), and System for Award Management (SAM) where a CO can see if a vendor is debarred or suspended.

- "Assessment" *could* also be something associated with a FedRAMP, SSAE-18 (e.g., SOC 1), or PCI DSS report.
- Be careful. If you point to an 800-53A-based (or similar) security controls assessment as the level of rigor, you are establishing a very expensive threshold for yourself; one that may now have to be met for every supplier you do business with.
- What is a level of "review" or "evaluation" that your organization can sustain? Do that.

Inspection of Systems or Components [SR-10]

For C-SCRM purposes, we associated “inspection” with something that takes physical form.

We had to draw some level of distinction, some limiting principle, between what we’d do for something we could view visually or optically versus things we do digitally like red team testing, vulnerability, or baseline scanning. The latter things are the next control.

OPM does do random inspections of physical components. However, referring back to Slide 9, this is going to be of limited value.

Sure, we have materiel about what to look for, a component inspection form, and all that, but this is not an area where we see a great deal of return on investment.

Component Authenticity [SR-11]

For C-SCRM purposes, this is for all non-physical things. Namely software.

At the post-acquisition but pre-implementation stage, we look to have assurance that the software gets to us from its point of distribution (usually a download) as intended. This is where techniques like out-of-band hashes, encryption, and digital signatures help us.

At the post-acquisition and post-implementation stage, we have lots of capabilities like EDR, baseline configuration scanning, SIEM capabilities, vulnerability scanning (many CVEs begin as underlying C-SCRM problems), and penetration and offensive testing.

In general, an organization's capabilities will be much stronger post-implementation than they will be pre-implementation.

Component Authenticity | Anti-counterfeit Training [SR-11 (01)]

Once again, referring back to Slides 9 and 15, this capability is going to be of limited value to most organizations.

Sure, we have training materiel, and we train our folks. But understand that, to be truly meaningful, anti-counterfeit training would need to be advanced and be delivered to well-experienced digital forensics analysts.

Open Forum