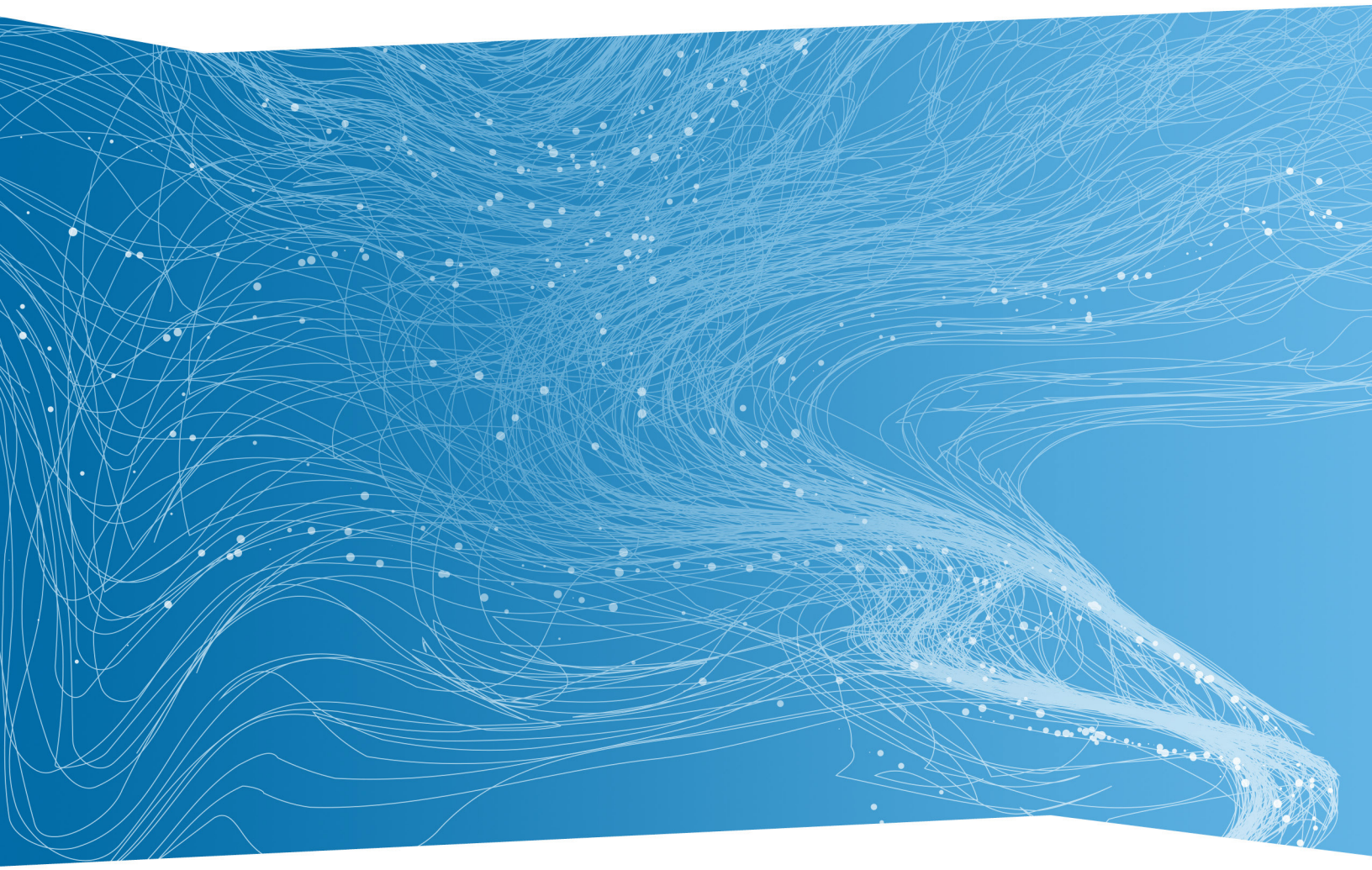
RSA



WHITE PAPER

3 REASONS TO ADOPT THE NIST CYBERSECURITY FRAMEWORK

RSA

Thinking about adopting the NIST cybersecurity framework?

If so, congratulations!

You're setting the stage for some impressive improvements in your organization's ability to manage cyber risk.

If not, why not?

Even if your organization isn't a federal agency that's required to implement the framework, you stand to gain a lot by adopting it anyway.

THE CASE FOR STATE AND LOCAL ADOPTION

Introduced in 2014 in response to Presidential Executive Order 13636 on improving the nation's cybersecurity,[1] the National Institute of Standards and Technology (NIST) cybersecurity framework received renewed attention in 2017, when Executive Order 13800 made it official federal policy.[2] Issued May 11, 2017, the order instructs federal agencies to adopt the framework to manage their cybersecurity risk. Strictly speaking, this order applies only to federal government agencies. But given the framework's stated purpose of improving critical infrastructure cybersecurity,[3] it has the potential to be a powerful force for positive change across a broad range of government and private-sector organizations, particularly critical-infrastructure organizations.

This paper is intended to make the case for state and local government organizations to adopt the NIST cybersecurity framework for a variety of reasons, chief among them to:

- *Improve critical infrastructure cybersecurity at local levels*, for organizations engaged in delivering essential services as described by the U.S. Department of Homeland Security[4]
- *Generally improve cybersecurity to manage the risk of cyber attacks*, regardless of whether an organization is part of the DHS-defined critical infrastructure
- *Strengthen cybersecurity processes to increase overall resilience* and avoid the negative operational and financial impacts of interruptions to the business of government

Even though adoption of the framework is not mandated by law the way compliance with NERC CIP, HIPAA, PCI and other regulations is mandated, the benefits make voluntary adoption by government and private-sector organizations both inside and outside the critical infrastructure well worth the effort.

RSA

FIRST THINGS FIRST: NIST CYBERSECURITY FRAMEWORK BASICS

NIST describes its framework for improving critical infrastructure cybersecurity as "guidance…to better manage and reduce cybersecurity risk."[3] It addresses the fragmentation that characterizes today's cybersecurity landscape by attempting to create a cohesive, unifying framework for cybersecurity. The framework proposes a common set of best practices and risk management principles that can be applied across a broad range of organizations.

The framework was developed through a joint effort of more than 3,000 people representing government, industry and academia. It centers on a core set of functions that are used to organize cybersecurity activities. These functions are to:

- *Identify* cybersecurity vulnerabilities
- *Protect* areas at risk by applying appropriate safeguards
- *Detect* cybersecurity events in a timely way
- *Respond* appropriately when an event is detected
- *Recover* normal operations after a cybersecurity event

Each function is further broken down into categories and subcategories of related tasks. For example, access control would be a typical task undertaken as part of the *protect* function. Activities in the core set of functions are concurrent, rather than serial or sequential, and they are intended to be part of a continuing effort to address cybersecurity risk.

WHAT DOES IT MEAN IN A PRACTICAL SENSE TO IMPLEMENT THE FRAMEWORK?

NIST has identified eight use cases[5] for leveraging the cybersecurity framework to address cybersecurity-related responsibilities. These suggest ways in which organizations can integrate the framework into work they're already doing to manage cybersecurity risk:

1. Integrate Enterprise and Cybersecurity Risk Management
2. Manage Cybersecurity Requirements
3. Integrate and Align Cybersecurity and Acquisition Processes
4. Evaluate Organizational Cybersecurity
5. Manage the Cybersecurity Program
6. Maintain a Comprehensive Understanding of Cybersecurity Risk
7. Report Cybersecurity Risks
8. Inform the Tailoring Process

In addition, the ability to identify gaps and to use the framework for reporting facilitates clear communication of critical information to executive leadership.

RSA

3 REASONS TO ADOPT THE NIST CYBERSECURITY FRAMEWORK

1. IMPROVE CRITICAL INFRASTRUCTURE CYBERSECURITY AT LOCAL LEVELS.

   For organizations that are part of the 16 critical sectors defined by the Department of Homeland Security as those whose incapacitation or destruction would have a debilitating effect on security, public health or other areas, adopting the NIST cybersecurity framework can help manage the risk of a cyber attack. The 16 sectors include several areas in which state and local governments commonly have operations—for example, emergency services, energy, financial services, healthcare, nuclear reactors, transportation and water/wastewater.

   Given that these are all highly regulated areas, it might seem reasonable to conclude that measures already being taken to comply with regulatory requirements will be sufficient to protect against the consequences of a cyber attack. In reality, the NIST cybersecurity framework may actually enhance, rather than duplicate, existing compliance-related efforts. In healthcare, for example, implementing the framework can help demonstrate due diligence in safeguarding protected health information as required by the Health Insurance Portability and Accountability Act (HIPAA).[6]

2. GENERALLY IMPROVE CYBERSECURITY TO MANAGE THE RISK OF CYBER ATTACKS.

   "Entrusted with the safety and protection of the public from a variety of threats, state and local governments must continuously develop their capabilities and knowledge of today's sophisticated cyber threats."[7] That was Cisco's position back in 2015, advocating for adoption of the NIST cybersecurity framework at local levels shortly after the framework's initial release. It's as germane as ever now, if not more so, as cybersecurity threats continue to grow. Moreover, its message applies broadly to all organizations at risk for threats like ransomware and other malware, phishing schemes, hacktivism or any of a number of other avenues of cyber attack—and not just those organizations that are part of the nation's critical infrastructure.

The NIST cybersecurity framework helps generally improve cybersecurity by introducing a common set of standards and best practices to cybersecurity strategies. Organizations that adopt it will find themselves better equipped to share information internally so that they can more effectively detect and respond to threats.

"The cybersecurity framework provides a baseline for all of our state agencies," the CIO of a populous Midwestern state told us. "That helps our centralized IT teams to analyze data and implement solutions that provide the greatest security impact across the state."

RSA

There's also the benefit of being part of the larger connected fabric of cybersecurity that the framework weaves. As *TechRepublic* has observed, "…the latest disasters seemingly come out of nowhere, and the reason why we're constantly caught off guard is simple: There's no cohesive framework tying the cybersecurity world together."[8] The NIST cybersecurity framework aims to change that.

3. STRENGTHEN CYBERSECURITY PROCESSES TO INCREASE OVERALL RESILIENCE.
   Beyond strengthening an organization's ability to protect constituents from the personal and financial harm that a cyber attack can inflict, the NIST cybersecurity framework also helps protect the organization itself against the potentially catastrophic consequences of interrupted operations, including the inability to deliver needed services to constituents.

By organizing cybersecurity processes within a straightforward context for action—*identify*, *protect*, *detect*, *respond and recover*—NIST has created a logical framework for implementation use cases (see p. 3) that will help increase cybersecurity and, in the process, strengthen resilience. Organizations that incorporate the framework into their cybersecurity strategy stand to reduce their chances of a cyber attack interrupting operations and, in the event there is an interruption, enhance their ability to return to normal operations.

NOW WHAT?

Organizations can begin immediately to lay the groundwork for adoption of the NIST cybersecurity framework by taking steps to assess where they are—and aren't—conforming to the framework's functional requirements (*identify*, *protect*, *detect*, *respond*, *recover*), and then starting from that baseline to strategize next steps. A wide range of security technology already exists that can support both pre-implementation and implementation:

- *Identify* areas at risk for cyber attack using governance, risk and compliance (GRC) solutions that automate identification of assets.
- *Protect* areas at risk with authentication solutions designed to ensure that people seeking access to critical assets are who they say they are.
- *Detect* cyber events and *respond* quickly with threat detection and response solutions that focus on reducing the time between when an attack commences and when it's detected.
- *Recover* normal operations with business resilience solutions that integrate incident response and crisis management.

Whether your organization is part of the federal government or not, or operating in a critical sector or not, consider adopting the NIST cybersecurity framework to help improve your cybersecurity posture—and protect you and your constituents from the consequences of a cyber attack.

RSA

ABOUT RSA ARCHER

Learn about RSA Archer® solutions for GRC, including RSA Archer Cybersecurity Framework Management App-Pack for managing cybersecurity based on NIST cybersecurity framework guidance, at rsa.com/grc.

ABOUT RSA

RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to rsa.com.

[1] "Executive Order—Improving Critical Infrastructure Cybersecurity," obamawhitehouse.archives.gov (February 12, 2013)

[2] "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," whitehouse.gov (May 11, 2017)

[3] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," v. 1. NIST.gov (February 12, 2014)

[4] U.S. Department of Homeland Security, "Critical Infrastructure Sectors," DHS.gov

[5] National Institute of Standards and Technology, "The Cybersecurity Framework: Implementation Guidance for Federal Agencies," NIST.gov

[6] Health Information Trust Alliance, "Healthcare Sector Cybersecurity Implementation Guide," hitrustalliance.net (October 2015)

[7] Cisco Systems and the Chertoff Group, "Addressing Critical Infrastructure Cyber Threats for State and Local Government," cisco.com (2015)

[8] Brandon Vigliarolo, "NIST Cybersecurity Framework: The Smart Person's Guide," TechRepublic.com (May 19, 2017)