Where Government & the NIST Cybersecurity Framework Meet

RESEARCH BRIEF

Symantec™ DLT®

Executive Summary

The National Institute of Standards and Technology (NIST) works to promote U.S. innovation and competitiveness by advancing science, standards and related technology through research and development in ways that enhance economic security and improve quality of life. To help the nation address its greatest information security challenges, NIST's cybersecurity programs seek to enable greater development and application of innovative security technologies. More specifically, NIST provides guidelines for federal, state and local agencies to help them address the nation's greatest challenges, like cyberthreats.

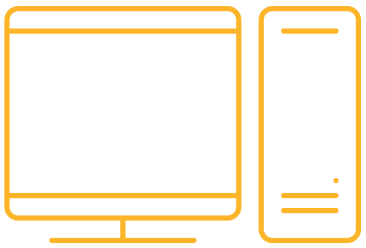
That's why, in 2014, the institute developed the NIST Cybersecurity Framework (CSF), which was created through collaboration between industry and government. The CSF consists of standards, guidelines and practices to promote the protection of critical infrastructure and improve government security.

To gauge how government is using the Cybersecurity Framework and its effectiveness, GovLoop partnered with Symantec, a leader in addressing advanced security threats, to survey 284 public-sector employees. The survey focused on the CSF's usage, perception and outcomes in government cybersecurity.

GovLoop also interviewed Kevin McPeak, Certified Information Systems Security Professional (CISSP) and Principal Cyber Architect for the Federal Sector at Symantec, to gain a better understanding of the survey results and specific ways government can use the Cybersecurity Framework to strengthen its cyber posture.

This research brief summarizes the findings of the survey while addressing how to get more agencies to adopt the CSF, as well as continuing cyber education and best practices.

Government's Cybersecurity Challenges



There are many challenges for government that demonstrate the need for the Cybersecurity Framework. These include rapidly evolving cyberthreats, unsecured legacy systems and serious mishandling of important government information.

Increasingly sophisticated cyberattacks continue to threaten government's greatest cyber defenses. There are cyberattacks capable of shutting down entire government infrastructures.

Take Distributed Denial of Service (DDoS) attacks, for example, which have increased over 125 percent year over year. DDoS attacks are malicious attempts to render a website or web application unavailable to users by overwhelming the site with an enormous amount of traffic, causing the site to crash or operate very slowly. While DDoS attacks are one of the oldest types of threats against websites, they are constantly evolving, making it harder to defend against them. Today, attackers use large armies of automated "bots" – computers that have been infected with malware and can be remotely controlled by hackers – to create DDoS attacks on a very large scale.

Even sophisticated personal devices like smartphones are attractive targets for online criminals, as more sensitive information is increasingly contained in these connected technologies. As new technologies and platforms develop, government will need to constantly reassess its own technology platforms to ensure they can still combat new and evolving threats.

And it's not just outside attacks that government has to worry about. Insider threats can also inflict serious damage, like the release of highly sensitive documents that could harm government's reputation, put employees at risk or expose the private information of citizens.

There are two types of insider threats: malevolent actors who deliberately sabotage government systems and unwitting actors who mishandle sensitive information.

Despite significant increases in cybersecurity awareness, including Presidential Executive Order 13587 – which provides structural reforms to improve the security of classified networks and the responsible sharing of classified information – there is no level of profiling that can predict insider threats with 100 percent effectiveness.

Finally, government is often constrained by legacy IT infrastructure that may hinder efforts to strengthen their overall cybersecurity posture. Approximately three-quarters of all government IT spending is going to support legacy systems (computer systems or technologies that are often out of date or need replacement). Despite cybersecurity being such a high priority for government, budgets continue to shrink. Such constraints force agencies to try to do more with less.

All of these cybersecurity challenges aren't going unnoticed at government agencies. At least 77 percent of recent GovLoop survey respondents said cybersecurity is a top priority at their agency (Figure 1). This is reflected by the fact that most respondents (74 percent) said their agencies plan on investing more resources (money, staff, etc.) in cybersecurity efforts in 2017 than the previous year (Figure 2).

But with such multifaceted cyber challenges and a variety of priorities to address, it can be difficult for agency leaders to even know where to start. That's where a framework can help.

Figure 1

What priority is cybersecurity at your agency?

HIGH PRIORITY (77%)
MEDIUM PRIORITY (17%)
LOW PRIORITY (4%)
NOT A PRIORITY (2%)

Figure 2

Will your agency invest more resources (money, staff, etc.) in cybersecurity efforts in 2017?

YES (74%)
NO (26%)

The NIST Cybersecurity Framework

To increase adoption of the Cybersecurity Framework, it's important for agency leaders to understand why the CSF came about and what it entails. "The NIST Cybersecurity Framework can really help government agencies better align their business needs with their missions and how they allocate their IT spending on cyber," Kevin McPeak said. "But it can be confusing for agencies because the origin was, to a large degree, a set of recommendations for critical infrastructure."

The safety and economic security of the nation depends on reliable critical infrastructure. To strengthen the resilience of this infrastructure, President Obama issued an Executive Order, "Improving Critical Infrastructure Cybersecurity," on Feb. 12, 2013. It calls for the development of a voluntary Cybersecurity Framework that provides a "prioritized, flexible, repeatable, performance-based and cost-effective approach: to manage cybersecurity risk for such processes, information and systems involved in critical infrastructure services."

The ties between cybersecurity and critical infrastructure are clear cut, as the internet and other IT infrastructures are vital to the nation. "Things like telecommunications, power grids and traffic control [all critical infrastructure] have everything to do with cybersecurity," McPeak said.

NIST's Cybersecurity Framework offers "a set of industry standards and best practices to help organizations manage cybersecurity risks." The CSF helps organizations, regardless of size or degree of cybersecurity risk, apply the principles and best practices of risk management to strengthen their cyber posture and increase the resiliency of critical infrastructure

The CSF provides five common guidelines to help organizations organize cyber priorities, including:

1. **Describe current cybersecurity posture**
2. **Describe a target state for cybersecurity**
3. **Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process**
4. **Assess progress toward the target state**
5. **Communicate among internal and external stakeholders about cybersecurity risk**

Additionally, the CSF is composed of three essential parts: the **framework core**, the **framework implementation tiers** and the **framework profiles**. Each component is meant to reinforce the connection between agency missions and cybersecurity activities, as described below:

Framework Core:

A set of cybersecurity activities, desired outcomes and applicable references that are common across critical infrastructure sectors. The core presents industry standards, guidelines and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization, from the executive level down to the operations level.

Framework Implementation Tiers:

A set of tiers to provide context on how an organization views cybersecurity risk and the processes in place to manage risk. Tiers describe the degree to which an organization's cybersecurity risk management practices reflect the principles of the Cybersecurity Framework (i.e. risk awareness, adaptiveness). The tiers range from partial (Tier 1) to adaptive (Tier 4).

Framework Profile:

The outcomes based on business needs that an organization has decided on. The profile can be seen as the alignment of standards, guidelines and practices to the CSF core in implementation scenarios. Profiles can also be used to identify opportunities for improving cybersecurity posture by comparing the current state profile to a target profile.

The document is meant only to complement, rather than replace, an organization's risk management process and cybersecurity program. Agencies without existing cybersecurity programs can also use the Cybersecurity Framework as a reference to establish their own procedures.

Ultimately, the CSF helps agencies identify opportunities to strengthen and communicate their management of cybersecurity risk while aligning with standard industry practices. It serves as a guide that agencies can use to navigate various cyber challenges, including evolving cyberattacks, legacy systems and insider threats. If understood and implemented properly, the CSF can help agencies be better informed, prioritize decisions regarding cybersecurity and plan accordingly.

The Need for Education

Figure 3

Does your agency leverage a security framework?

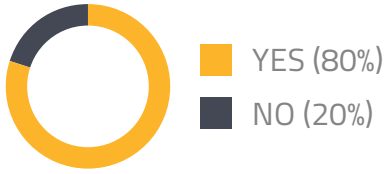
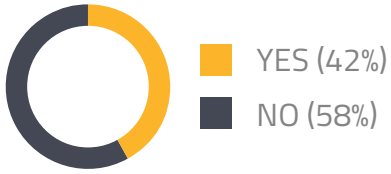


Figure 4

Do you know what the NIST Cybersecurity Framework is?



Despite cybersecurity being a top priority for government and the usefulness of a guide with standards and best practices, many government employees don't even know about the NIST Cybersecurity Framework. The majority of survey respondents (80 percent) said their agency leverages at least some type of security framework (Figure 3). However, of those who do not leverage a cybersecurity framework already, 58 percent of respondents said they were not aware of the CSF (Figure 4).

The survey results demonstrate a clear need for increased awareness surrounding the CSF. McPeak said the lack of understanding and adoption could be due to misperceptions around the CSF's applications. "Some may think their jobs aren't necessarily associated with it," he said. "That's why communication is really important. People just need to better understand how useful it is. It's not just a 'nice to have,' it's a 'must have.'"

Additionally, many public servants believe NIST's Cybersecurity Framework is only applicable to critical infrastructure missions. Conversely, some employees working on critical infrastructure issues think that the CSF has nothing to do with their specific function because they don't have any cybersecurity responsibilities. As McPeak pointed out earlier, however, the CSF can be applied to non-critical infrastructure jobs and settings because of the importance of IT to any mission, while cybersecurity is crucial to ensuring critical infrastructure programs (like power grids and telecommunications) are protected and function properly.

Education is required to help employees understand how the CSF can be applied to any role or agency mission. The first step to promoting awareness of the Cybersecurity Framework is to increase training within your agency. While this seems obvious, it is difficult for many leaders to prioritize this investment when faced with shrinking budgets and competing priorities. That's where security awareness web-based training can be useful.

Web-based security training modules are online educational sessions that can be easily integrated into your agency's learning system. Department leaders can then customize the training, provide communications tools and deliver other services that meet the agency's particular security awareness needs and goals.

Employees, regardless of level, should be aware of the reality of threats, vulnerabilities and consequences and have the information needed to help them take active roles in securing the agency's enterprise information. Security awareness web-based training can help educate employees on many of today's key cybersecurity issues, including information protection, social networking, virus protection, password security, web-browser security, email security and mobile security.

It also provides actionable steps. A successful security awareness program influences attitudes and behavior. It instills and reinforces safe practices and security habits so they become part of daily tasks and interactions. Ideally, your agency's security awareness program should:

1. **Promote employee awareness that everyone is responsible for organizational security.**
2. **Teach the security principles for which employees are responsible.**
3. **Raise employee awareness of the cyberthreats in the agency's landscape.**
4. **Teach how to apply the security principles to everyday tasks.**
5. **Remind, refresh and update the security principles and best practices learned.**

A large component of the NIST Cybersecurity Awareness Framework is cyber awareness and training. But without a core security training program that raises awareness about the importance of cyberthreats and safe cyber practices employees can use, it is unlikely that the CSF would be of any use to an agency.

"Communication is really important. People just need to better understand how useful it is. It's not just a 'nice to have,' it's a 'must have.'"

Kevin McPeak,
Certified Information Systems Security Professional (CISSP) and Principal Cyber Architect for the Federal Sector at Symantec

CSF Usage

While many agencies lack education and awareness around the CSF, there are also many government IT departments proactively using the NIST Cybersecurity Framework. Of survey respondents whose agencies do employ any type of framework, 62 percent said they use the CSF (Figure 5). However, most have yet to implement all the recommendations nor do they plan to do so within the next year.

Of respondents who do use the NIST Cybersecurity Framework, 60 percent have implemented some of the recommendations while only 39 percent have implemented all of the recommendations (Figure 6). Only 38 percent of respondents who do not yet follow the CSF say their agencies plan to implement it in the next 12 months (Figure 7).

"This isn't cause for alarm," McPeak said. He stressed the importance of recognizing cybersecurity as an ongoing process. "You have to build toward it," he said. "Many agencies are probably not where they want to be yet, but as you gradually improve your strategy, your cyber posture will also improve."

One way to continue that journey is to break the CSF into more easily relatable pieces. A five-function strategy can help strengthen your cyber posture. The functions include prepare/identify, protect, detect, respond and recover. When you narrow the CSF's many components down to these functions, you can evaluate each one as part of your organization's overall cybersecurity strategy and posture.

For example, consider the first function, prepare and identify. Vulnerability assessments can expose weaknesses in an organization's security posture. By evaluating the risk posed by each weakness and addressing the concerns that are most critical, IT leaders can improve agency preparedness for an attack. With each scheduled cycle of assessments, agencies can hone their security strategies according to their individual needs.

By laying out a detailed but simpler strategy, agency leaders have a better chance of implementing the actual recommendations of the CSF. In contrast, simply trying to apply a sophisticated and complex framework can cause significant confusion, discouraging any agency from sticking to the principles and following through on the recommendations.

To make the most of the five functions strategy and prepare your agency to implement the CSF, use these best practices as guidelines:

1. **Improve** visibility and understanding of your information and systems through asset and network discovery as well as mapping.
2. **Protect** your agency's endpoints and gateways from targeted attacks and advanced threats while protecting your mobile workforce and end user data.
3. **Detect and respond** accordingly to cyberthreats by having the big data and analytic tools in place. Strengthen this practice by using cloud and mobile solutions to help process and analyze structured and unstructured cybersecurity-relevant data.
4. **Create** a plan and outline how your agency intends to respond to cyber incidents. Determine how response processes and procedures will be maintained and tested.
5. **Develop and implement** the appropriate systems and plans to restore any data and services that may have been impacted during a cyberattack.

Once your agency starts improving its cyber posture, agency leaders are more likely to understand what is laid out in the CSF and direct priorities. More importantly, your agency will be more likely to successfully follow through on the recommendations and implement them accordingly.

Figure 5

Does your agency leverage the NIST Cybersecurity Framework?

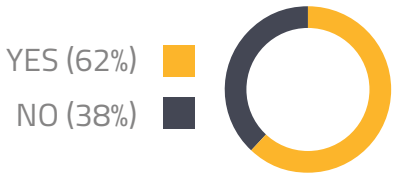


Figure 6

Have you implemented all of the NIST Cybersecurity Framework's recommendations or just some?

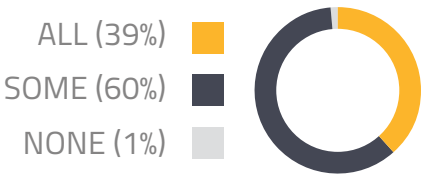
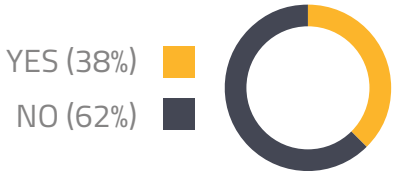


Figure 7

Does your agency plan to implement the NIST Cybersecurity Framework in the next 12 months?



Ensuring Successful Outcomes

Having a cyber framework in place yields many benefits for agencies, particularly in knowing where to start combating cyberthreats or implementing recommendations. While following NIST's recommendations does not necessarily guarantee elimination of cyberthreats, it will significantly improve an agency's cybersecurity posture.

Survey respondents agreed. Sixty-eight percent of survey respondents said their confidence levels in the Cybersecurity Framework were high (Figure 8), while 85 percent believe that using the CSF will help reduce their cyberrisk (Figure 9).

In addition to better security, agencies can reap other benefits by leveraging the CSF, including decreased costs, better prioritizing of resources and reduced redundancies.

A big part of successful CSF outcomes is using the right tools. "You want to make sure you're matching your solution to your agency's specific needs," McPeak said. "You can then identify where you have redundant solutions in place and clarify what you have and what you're missing. That way, you can streamline efforts and reduce your total costs by identifying what you really need to spend money on."

In addition to education and strategy, agencies need the right tools to help ensure successful CSF implementation and outcomes. Solutions like Advanced Threat Protection (ATP) platforms can help you visually map out your IT environment and where you need to prioritize resources based on your agency's mission. Such platforms can help uncover, prioritize, investigate and remediate advanced threats across multiple control points from a single console.

An agency can streamline its efforts and save on costs by prioritizing anomalous events, allowing security analysts to focus on what matters most. IT leaders can uncover stealthy threats that others miss by leveraging large civilian threat intelligence networks. Incident responders are then notified as soon as an organization has been identified as a target of an active attack campaign.

ATP platforms can help agencies carry out these practices to better guarantee successful outcomes:

1. **Detect, prioritize, investigate and remediate** threats across multiple control points in a single console.
2. **Uncover** stealthy threats across end-points, network, email and web traffic.
3. **Prioritize** what matters most by correlating across events from all control points for complete visibility and faster remediation.
4. **Contain and remediate** any potential cyberattack in minutes, with a single click.

Ultimately, with ATP, your agency can better repair any gaps in its cyber defense. Whatever you may have overlooked or not properly allocated enough resources toward, ATP can help you better detect and remediate such gaps.

Paired with ATP, the CSF can help agencies apply more focus on critical areas, based on individual agency mission requirements. Agencies can achieve better return on investment knowing that they are not just throwing money aimlessly into components of their IT infrastructure that are not critical to the agency or vulnerable to threats.

Figure 8

What is your confidence level in the NIST Cybersecurity Framework to improve your agency's cybersecurity posture?

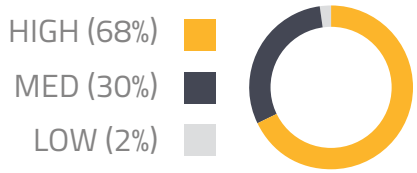
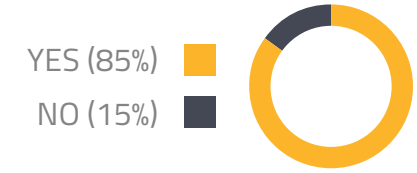


Figure 9

Do you believe that using the Framework has reduced or will reduce your cybersecurity risk?

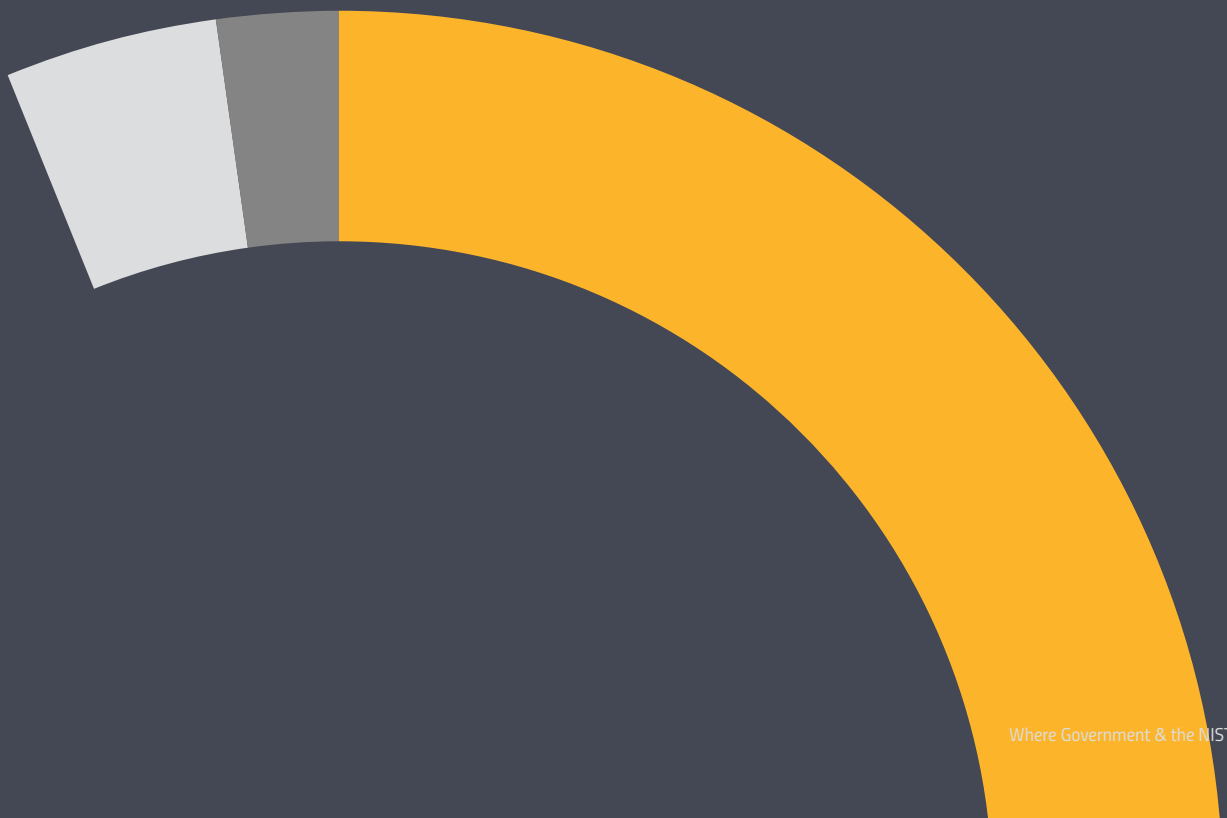


Conclusion

Ultimately, the NIST Cybersecurity Framework is highly valuable to government, but only if agency leaders and employees alike know how to leverage it.

The GovLoop survey results show that there's still work to be done in increasing awareness of the Cybersecurity Framework in addition to more guidance for best practices and implementation.

Fortunately, confidence in the CSF is high. To guarantee better outcomes, agencies should look to solutions like web-based security training to improve employee awareness, training and cyber education; a standard cyber strategy like the five functions to help agencies better implement recommendations and advanced threat protection to help agencies better identify their most critical threats and use resources accordingly.



About Symantec

Symantec helps federal agencies develop and implement comprehensive and resilient security strategies to reduce risk and meet Cross-Agency Priority Goals, the NIST Cybersecurity Framework, the Joint Information Environment and other federal mandates. To learn more visit www.symantec.com.

About DLT Solutions

For 25 years, DLT Solutions has been dedicated to solving public-sector IT challenges. Guided by our relentless focus, we have grown to be one of the nation's top providers of world-class IT solutions. Leveraging our strategic partnerships with top IT companies, we develop best-fit solutions for our federal customers.

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW, Suite 800
Washington, DC 20005

(202) 407-7421
F: (202) 407-7501

www.govloop.com
@govloop