Justice Guardian - Navigating Cybersecurity:
Protect Core Function, NIST Cyber Security Framework *for Command Staff*

What Is It?

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF) provides high-level cyber security objectives, structured around six Core Functions: Govern[1], Identify, Protect, Detect, Respond, and Recover, that aid agencies in understanding, assessing, prioritizing, and communicating their protection efforts.[2] Protect, is the third Core Function and the final one that focuses on safeguards to manage the organization's cybersecurity risks.

Image credit N. Hanacek/NIST.

Why Does It Matter?

The Protect function supports an organization's ability to secure their assets (data and infrastructure) by reducing the likelihood and impact of adverse events, while simultaneously increasing an organization's ability to successfully take advantage of opportunities. Building off Identify's efforts to align cybersecurity activities with business objectives, organizations are able to implement solutions that will aid in identity management, authentication, and access control; awareness and training; data and platform security; and resilience.

What to Do

Protect is a technical function that will require careful implementation over several years, to move the organization to the target cybersecurity profile. It is worth noting that the profile will continually adapt as Command Staff review the decisions and actions from Govern and Identify. Five Categories are key to implementation.

- Identity Management, Authentication, and Access Control limits physical and logical access to authorized entities. Terminology such as "zero trust" is common to the processes and technologies in this category.
- Awareness and Training is for both general staff and those with functions that require additional protections, such staff involved in digital evidence and sensitive transactions involving protected data, such as criminal justice information, financial transactions, and personnel data.
- Data Security includes efforts to ensure the confidentiality, integrity, and availability of data. This Category includes the all-important function of data backups, which are one of the only ways to mitigate ransomware incidents.
- Platform Security provides for the confidentiality, integrity, and availability of hardware, software, and physical and virtual platforms. It is an often-trivialized component of cybersecurity and safeguarding Criminal Justice Information Services (CJIS).
- Technology Infrastructure Resilience stresses the ability of networks and platforms to maintain availability during normal and adverse conditions.

Considerations

Protection is an ongoing effort that must evolve as threats and vulnerabilities change but do not be lured in by the promise of "artificial intelligence" (AI)-powered technologies. It is important to start with a solid foundation before moving on to tools that integrate developing concepts. Keep in mind that command staff leadership in and support of changes is critical - nothing can derail improvements faster than ignoring or tolerating workarounds. Although data and platform confidentiality is meant to include privacy considerations, justice sector organizations should provide extra consideration to how citizens will interpret the privacy aspects of any implementation.

Further Reading & Resources

- NIST provides both brief explanations of the Core Functions and detailed information (e.g., Protect).
- As ransomware remains a high priority threat to justice agencies, there is a NIST Getting Started with Cybersecurity Risk Management guide specifically for Ransomware.

---

[1] The Govern Core Function is new to version 2.0 and moves multiple subcategories to new Core Functions.

[2] This Justice Guardian builds on the information provided in the Justice Guardian series: "Determining a Framework," Govern, and Identify which should be read first.

Justice Guardian - Navigating Cybersecurity:
Protect Core Function, NIST Cyber Security Framework *for Technical Implementors*[3]

Technical Insight
Implementation of the Protect Core Function is almost entirely dependent on technical staff. Cybersecurity professionals will recognize numerous familiar concepts among the Protect Categories and sub-categories, including the Confidentiality, Integrity, and Availability (CIA) triad, zero trust, least privilege, identity and access management (IAM). Although the CSF may use more generic terms in some instances, the fundamental concepts remain the same.

Technical Details
Common language and concepts of the five Categories are listed below. These terms are not necessarily the most important in each Category but are the ones that will be commonly recognized by cybersecurity practitioners.

- Identity Management, Authentication, and Access Controls – zero trust architecture; IAM; cryptographic key and token management; principles of least privilege and separation of duties; and (identification) authentication, authorization, and accountability (AAA/IAAA).
- Awareness and Training – cyber hygiene and user assessments, including exercises.
- Data Security – CIA triad for data at rest, in use, and in transit; encryption; digital signatures; cryptographic hashes; data loss prevention; use of production environments; and secure, off-site, tested, and maintained back-ups.
- Platform Security – CIA triad for hardware, software, and physical and virtual platforms; patching, updating, and replacing; end-of-service/-life; logging and log review; and allow- and/or block-listing.
- Technology Infrastructure Resilience – segmentation (e.g., IT, IoT, OT, mobile, guests) and single-direction paths; zero trust architecture; focus on all threats inclusive of accidental, structural, environmental, and adversarial; off-site operations (e.g., hot/warm/cold sites); and single points of failure.

What To Do
Many of the tasks within Protect are addressed by questions in the Cyber Security and Infrastructure Agency's (CISA) and NIST sponsored National Cybersecurity Review (NCSR), run by the Center for Internet Security (CIS). Tools listed under CISA's Cybersecurity Performance Goal: Protect and CISA-vetted tools freely available to government agencies under the Services and Tools list can provide an agency a jumpstart in completing this function.

Technical Considerations
Existing frameworks and regulations, including CSF 1.1, and NIST publications are already cross-walked to NIST CSF 2.0. Using these crosswalks can assist with implementation if a different framework or regulation was previously in use, but also to help understand complex topics and align with major privacy frameworks, such as the California Privacy Rights Act.

Further Reading & Resources

- National Cybersecurity Review (NCSR)
- The National Online Informative References Program (OLIR) standardized online informative references (OLIRs) between elements of their documents, products, and services and elements of NIST documents.

[3] This page builds on the information provided in the "for Command Staff" document.