Justice Guardian - Navigating Cybersecurity:
Govern Core Function, NIST Cyber Security Framework[1] *for Command Staff*

What Is It?
The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[2] provides high-level cybersecurity objectives, structured around six Core Functions (Govern[3], Identify, Protect, Detect, Respond, and Recover) that aid agencies in understanding, assessing, prioritizing, and communicating their efforts. The Govern Core Function, new to v2.0, consists of administrative tasks to "establish and monitor the organization's cyber security risk management strategy, expectations, and policy."

Image credit N. Hanacek/NIST.

Why Does It Matter?
Much like a standard risk management exercise, Govern ensures that the agency's internal and external people, processes, and technologies are understood within the context of its priorities, capabilities, constraints, risk tolerance, and legal and regulatory requirements. This enables the agency to create a thorough, fiscally sound, and proactive approach to minimizing cyber risks, while simultaneously increasing compliance with laws and regulations, improving decision-making during and after incidents, and promoting safety.

A byproduct of building a formal governance program is that it can be used to help secure future budgets, grants, and other funding avenues earmarked for technology and cyber security.

What To Do
Determine who in the agency is best positioned to lead the development of a cyber risk management strategy; i.e., someone already responsible for managing Criminal Justice Information System (CJIS) policy audits or the risk management program. At a minimum, the strategy will need to identify and document: 1) the organization context, including the mission, expectations, and requirements; 2) priorities, constraints, risk tolerance and appetite statements, and assumptions; 3) the cyber supply chain; 4) roles, responsibilities, and authorities; and, 5) establish, communicate, enforce, and improve cyber security policies, processes, procedures, and activities.

It is highly likely that a risk management plan already exists, which should have the cyber security risk management plan incorporated. Empower the team leader to make operational decisions and engage different departments to help accomplish these tasks. For instance, the team will need to answer questions such as "Is this a risk we can accept?" and "In the event of a complete network loss, in what order will systems be brought back online?"

Considerations
NIST CSF includes Framework Implementation Tiers (Partial, Risk Informed, Repeatable, and Adaptive) which "provide context on how an organization views cyber security risk and the processes in place to manage that risk." The Tiers are discussed in greater detail in Section 2.2. of NIST CSF v1.1, pages 15 - 18 of the PDF. Before working on tasks within Govern, review these Tiers and decide what and how quickly the agency should achieve it. Smaller agencies may choose to stop at Tier 3: Repeatable, based on their resources and risk.

Further Reading & Resources
- NIST CSF 2.0 Reference Tool is designed to provide a high-level, bulleted understanding of the Core Functions' Categories and Subcategories, with examples.

Cyber risk management is not redundant. It provides insights into the agency's hardware, software, and systems which experience different risks than purely physical equipment – details that are not documented elsewhere.

[1] This Justice Guardian builds on the information provided in "Justice Guardian - Navigating Cybersecurity: Determining a Framework," which should be read first.
[2] https://www.nist.gov/cyberframework
[3] The Govern Core Function is new to version 2.0 and moves multiple subcategories to new Core Functions. This document follows the draft version of 2.0, as of January 2024, and will be updated when the final version is released.

Justice Guardian - Navigating Cybersecurity:
Govern Core Function, NIST Cyber Security Framework *for Technical Implementers*[4]

Technical Insight
Govern mostly consists of administrative tasks. However, these tasks require expert knowledge of the hardware, software, and stored data, which places the technical implementers in key positions to share issues and concerns with existing environments, practices, and contracts. "You can't protect, what you don't know."

Technical Details
CSF Profiles are documents designed to aid practitioners with aligning the requirements, risk tolerance, and resources of the agency to the Core Functions. Currently, the Profiles are based on v1.0 and v1.1 of CSF, but they may provide a useful starting point for understanding how to complete the Govern Core Function. Some of the profiles address technologies used by justice agencies, such as connected vehicle environments, maritime, and payroll profiles, while others address common threats, such as ransomware, botnet, and distributed denial of service (DDoS) threat mitigation profiles.

What To Do
Many of the tasks within Govern are addressed by questions in the Cyber Security and Infrastructure Agency's (CISA)[5] and NIST-sponsored National Cybersecurity Review (NCSR), which can provide a jumpstart in determining which areas of the Govern Core Function require more focus. Open from October through the following November, NCSR is a no-cost, anonymous, annual self-assessment for states (and agencies), local governments (and departments), tribal nations, and territorial (SLTT) governments.

Technical Considerations
Depending on the agency's locality, adhering to the CSF may be mandated. Since the CJIS policy (v5.9.1)[6] aligns with NIST 800-53r5[7] "Security and Privacy Controls for Information Systems", it is highly likely many tasks are already completed. This is where the National Online Informative References Program (OLIR) becomes invaluable with its Derived Relationship Analysis Tool that automates the process of comparing different standards. Existing OLIR documents provide a relationship mapping between 800-53r5 to the CSF v1.1

Additional Help
Numerous templates are available to assist in the risk management, policy, and procedure development process. Check the following locations for copies of their documents: 1) State agencies; 2) CSF Risk Management Resources; 3) SEARCH.org's Templates Resource; 4) International Association of Chiefs of Police Resources; and 5) SANS Security Policy Templates.

Further Reading & Resources
- CISA provides Public Safety agencies with cyber risk assessment tools and information in the "Guide to Getting Started with a Cybersecurity Risk Assessment." CISA risk management resources are here.
- Federal Virtual Training Environment (FedVTE) provides a wide range of on-demand courses related to the tasks in Govern. Anyone new to cyber risk management can begin with the 6-hour course "Fundamentals of Cyber Risk Management" and graduate to more complex topics. Access is free for any federal or SLTT government employee or veteran.

A cyber risk management plan provides a crucial foundation for implementing the rest of CSF. Technical guidance during this Core Function will ease the implementation of follow-on tasks.

[4] This page builds on the information provided in the "for Command Staff" page.
[5] https://www.cisa.gov/
[6] https://www.fbi.gov/file-repository/cjis_security_policy_v5-9-1_20221001.pdf/view
[7] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf