# Justice Guardian - Navigating Cybersecurity: Determining a Framework
## *for Command Staff*

### What is it?

A cyber security framework is a set of documents describing actions, guidelines, standards, and best practices to improve cyber security risk management. Implementing a cyber security framework allows an agency to follow a structured approach developed by teams of international experts. The four most common frameworks are:

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF)** – this framework is popular in government agencies as it was designed for critical infrastructure and provides a detailed series of high-level cyber security objectives that aid agencies in understanding, assessing, prioritizing, and communicating their efforts. Some federal, state, and local laws require agencies to adhere to NIST CSF, with grant funding tied to CSF – based tasks.
- **NIST 800 series** – these Special Publications (SP) documents provide technical details in how to implement cyber security for specific devices, applications, or environments. As of 2021, the Criminal Justice Information Security (CJIS) Policy (v5.9.1) began to align to 800-53r5 “Security and Privacy Controls for Information Systems.” It is important to note that there is no CJI security requirement to specifically implement 800-53r5.
- **International Organization for Standardization (ISO) 27001 and 27002** – these are detailed, technical standards for information security management and primarily used outside the United States and in international companies.
- **ISACA Control Objectives for Information and Related Technologies (COBIT)** - this framework addresses how to minimize business risks, technical issues, and control requirements and is often used in the financial sector.

### Why does it matter?

Each cyber security framework is slightly different in purpose and scope, but all reduce risk and increase security. Due to government and regulatory requirements for justice agencies, it is important to carefully consider and choose which framework is most complementary with your needs and resources, which might include maintaining compliance, passing audits, prevent data leaks, minimizing downtime, and allocating resources in the most effective way possible.

### What to do

Determine the framework that your agency will follow and begin aligning your cyber security operations to it, following the framework’s instructions. **The IJIS Cyber Security Task Force recommends the use of NIST CSF** as it provides a higher-level approach that is easier for many agencies to implement and can be mapped to NIST 800-53r5, the CJI Security Policy, ISO 27001, and COBIT.

### Considerations

Moving to align with any cyber security standard is a process that will take years to achieve. The most successful approach involves implementing the easiest and fastest controls first. For example, part of the Identify Core Function is to identify and document critical processes, assets, and information flows – it’s highly like this has already been accomplished as part of other projects and can be a “quick win.” As you move forward with determining a framework to implement:

- Involve senior officials and command staff as they will be able to help minimize disruption caused by changes and encourage a positive culture where cyber security is viewed as a critical element of operations.
- Use the Identify stage to understand how implementation will impact payroll and record management systems, service providers, and other agencies.
- Explore grants by Bureau of Justice Assistance (BJA), Federal Emergency Management Agency (FEMA), and the Cyber and Infrastructure Security Agency (CISA) that can be used for cyber security upgrades.

### Further Reading & Resources

- NIST CSF Getting Started Guide: https://www.nist.gov/cyberframework/getting-started
- International Association of Chiefs of Police Law Enforcement Cyber Center: https://www.iacpcybercenter.org/

***An ounce of prevention is worth a pound of cure.*** Cyber attacks will happen. Strengthening your cyber security ensures protection for your agency, officers, and staff; safeguards your sensitive information; allows for continued access to CJIS; and minimizes the loss of trust that occurs when an agency is a crime victim.

# Justice Guardian - Navigating Cybersecurity: Determining a Framework
## *for Technical Implementors*

**Technical Insight**

Choosing which cyber security framework to implement is an administrative choice that needs to be based on the current cyber security environment in a network and the needs of a particular agency.

**Technical Details**

- **NIST CSF** – this framework is structured around five Core Functions: Identify, Protect, Detect, Respond, and Recover. Designed to complement, not replace, existing security practices, the CSF provides insight into how to decide the right cyber security maturity level for a particular agency based on risk management decisions and then which components are most critical in implementing that approach. The CSF is one of the easiest frameworks to understand as it approaches the topics in general terms, rather than a highly technical format. As some laws require agencies to adhere to NIST CSF it is important to determine whether that is true for your agency or not.
- **NIST 800 series** – these are almost 200 SPs that provide highly technical details regarding the implementation of a specific aspect of cyber security. While adhering to 800-53r5 is extremely beneficial, there is little guidance as to which controls are the most important and when to move on to another SP. Even though the CJI Security Policy has begun to align to 800-53r5, nothing mandates its use as most requirements are included in the other frameworks, too.
- **International Organization for Standardization (ISO) 27001 and 27002** – these are highly detailed and technical documents. Unlike NIST CSF and NIST 800 series, there is a cost involved with purchasing the documents. However, it is possible to be ISO 27001 certified, which may be a local requirement.
- **COBIT** - this framework approaches cyber security from the aspect of meeting stakeholder needs, covering the enterprise, and using a single framework and holistic approach that separates governance from management. This is strongly oriented toward business management rather than technical implementation.

**What to do**

Determine and recommend to senior leadership and/or Command Staff the cyber security framework that best fits your agency's culture, environment, threat and risk appetite levels, existing cyber security maturity levels, and mandatory compliance drivers. For instance, an agency that has already completed many of the CSF tasks may find it more useful to move to 800.53r5, where as an agency that is just beginning its cyber security framework journey will find CSF more useful.

**Technical Considerations**

- When discussing the appropriate framework for use in a particular agency, know what type of data on the network must be protected; what infrastructure is critical to operations; if confidentiality, integrity, or availability is the most critical for that data type or infrastructure; and any specific data protection requirements. For instance, besides CJIS information, the agency will likely have personal health information (PHI), tax information, and credit cards stored on the network, all of which are also protected by other regulations.
- Do not hesitate to supplement one framework with information from another. For instance, while the CSF may provide some implementation and metric details, 800.53r5 can provide additional ones.

**After the Decision**

After choosing the appropriate framework, there are a multitude of free training classes and resources available to provide information on how to begin implementation. Many other justice sector security teams are also

**Further Reading & Resources –**

- CISA provides a public safety communications and cyber resiliency Toolkit.
- The Cyber and Infrastructure Security Agency (CISA) makes available a large number of trusted, free CISA and vendor resources that can be implemented for "quick wins."
- If your agency is not already a member of the Multi-State Information Sharing and Analysis Center (MS-ISAC), consider joining this free-to-you resource, funded by CISA.

**Cyber security initiatives provide immediate returns.** Choose to implement one high priority change at once, starting with the "quick wins" that build momentum and complement existing security components.

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