FORTRA™

WHITE PAPER (DIGITAL GUARDIAN)

Leveraging Digital Guardian to Support the NIST Cybersecurity Framework

Executive Summary

Developed in response to Executive Order 13636, the NIST Cybersecurity Framework (the "Framework") was published in February 2014 following a collaborative process between industry, academia and government organizations. The original goal was to develop a voluntary framework to help organizations manage cybersecurity risk in the nation's critical infrastructure, such as bridges and the electric power grid. But the framework has been widely adopted by many types of organizations across the country and around the world. Organizations that have adopted the Framework have found it to be an extremely valuable tool for fostering communications about risk management and cybersecurity amongst organizational stakeholders.

NIST defines the Framework as guidance, intended to be customized by various sectors and individual organizations to best suit their risks, situations, and needs. The Framework is not intended to be implemented as a static compliance checklist but rather a flexible, ongoing process and risk management tool.

The Framework's Core five "Functions" offer a way to organize cybersecurity risk management activities at their highest levels using words that can be applied across risk management disciplines: **Identify, Protect, Detect, Respond, and Recover.**

This white paper explains how federal organizations can leverage Fortra™'s Digital Guardian®'s the Data Protection Platform across these five Functions to more effectively implement eight strategic objectives of the Framework.

Reference https://www.nist.gov/cyberframework/questions-and-answers#basics

#1: Integrate Enterprise & Cybersecurity Risk MGMT

Using the Cybersecurity Framework's Functions (Identify, Protect, Detect, Respond, and Recover) as the basis for risk management dialogs, organizations can raise awareness of cybersecurity and other risks to be managed and facilitate communication among agency stakeholders, including executive leadership.

How the Digital Guardian Platform Can Help

- **Identify.** Digital Guardian (DG) enables organizations to learn where sensitive data is located, how it flows in the organization, and where that data is at risk. It can provide digital asset management and visibility into business process and workflows. DG incorporates and leverages requirements of various business units, including personnel, InfoTech, and Security. DG recognizes the hard and soft business processes, and provides the ability to organize this information into the Framework across extensive enterprise environments.
- **Protect.** Digital Guardian provides flexible protection and enforcement of data policies and rules protecting Organizations as the Cybersecurity Framework evolves over time.
- **Detect.** By providing visibility into all data, user and system events, and providing the ability to alert on any event, Digital Guardian allows near real time detection of incidents.
- **Respond.** Remediation capabilities are available throughout Digital Guardian solutions, including continuous education as well as confirmation of potential security exposures.
- **Recover.** Organizations need to understand which specific systems and what data has been exposed to confidently measure recovery. DG provides the forensic analysis required for identifying leakage and compromises, enabling validation of recovery procedures.

#2: Manage Cybersecurity Requirements

Federal organizations can use the Cybersecurity Framework Core Subcategories to align and reconcile cybersecurity requirements applicable to their organizations. This reconciliation of requirements helps to ensure compliance and provides input in prioritizing requirements across the organization using the subcategory outcomes. This capability becomes a means of operationalizing cybersecurity activities and a tool for iterative, dynamic, and prioritized risk management for the agency.

How the Digital Guardian Platform Can Help

- **Identify.** DG can identify and provide visibility into all user, system and data activities. This information can be used across all domains of security infrastructure to improve and confirm the efficacy of the operational tools.

- **Protect.** DG identifies anomalistic and intrusive behaviors allowing detection and protection of threats as the enforcement element of risk management policies.
- **Detect.** DG identifies how business is using data, potential policy conflicts, conflicting or unknown business processes empowering the agency to determine in-scope versus out of scope policies. For example, DG detects and alerts on potential incidents to all responsible organizational business units allowing for fact-based policy decisions.
- **Respond.** By helping to identify policy conflicts, overlaps or gaps, DG provides powerful intelligence specific to critical data and files needed for effective response.
- **Recover.** DG provides the details of last known state of a recoverable file. DG can support the prioritization of requirements across an organization by leveraging deep visibility, workflow and last known file and system states, empowering the agency with immediate focus on where to begin the recovery process.

#3: Integrate & Align & Acquisition Process

For acquisitions that present cybersecurity risks, federal organizations can choose to do business only with organizations that meet minimum cybersecurity requirements in their operations and in the products and services they deliver. Cybersecurity Framework Profiles can be used by federal organizations to express technical requirements; offerors can demonstrate how they meet or exceed these requirements.

How the Digital Guardian Platform Can Help

- **Identify.** Cybersecurity specialists recognize that data, systems and users are frequent targets of cyber criminals and nation state actors. Digital Guardian provides users with the unique ability to monitor these elements at the point of use. This enables security practitioners to demonstrate and report gaps in security, which gives federal organizations the opportunity to align acquisitions with current risks exposures.
- **Protect.** Digital Guardian extends cybersecurity protections beyond the perimeter for a mobile workforce, by providing either blocking or auditing of events for procedural violations such as data leakage, as well as suspicious system behaviors and activities.
- **Detect.** DG can establish user trends to baseline normal behavior over short and extended timeframes enabling the organization to determine if policy and procedural changes are effective in protecting sensitive digital assets.
- **Respond.** Visibility into the behavior of systems and service providers based on trend analysis over time provides a measurable indication of risk due to improperly aligned cybersecurity procedures. Trend data reporting and anomaly detection is based on standard deviations. These visual indicators provide business units with metrics needed to identify and adjust to a changing environment.
- **Recover.** By providing a full forensic record of all activity since a breach, DG enables organizations to restore data to its last known good state

#4: Evaluate Organizational Cybersecurity

Implementation Tiers provide organizations a basis for rationalizing various modes of cybersecurity operations across an organization, based on trade-off analysis of agency business units or specific assets. Gap analysis between the current and Target Implementation Tier will reveal opportunities for prioritizing cybersecurity investments.

How the Digital Guardian Platform Can Help

- **Identify.** Digital Guardian provides visibility into the work and data flow of business processes allowing the organization to make strategic decisions on efficacy of current products in their environment and incorporating metrics from DG to validate and substantiate current risk and exposures.
- **Protect.** Digital Guardian ensures protection of exposed sensitive data by providing deep visibility reporting that can help align of cybersecurity and data usage with business processes.
- **Detect.** DG can provide gap analysis through baselining, trending, and ongoing analysis of data

movements. Trending analysis is commonly used as the basis for anomaly detection.

- **Respond.** By understanding how data and systems are being accessed by users, reports can be shared among various business units enabling fact-based decision making and policy adjustments
- **Recover.** DG provides the last line of defense, protecting data exposures and recording all incidents.

#5: Manage the Cybersecurity Program

The core taxonomy of cybersecurity outcomes in Subcategories provides a way to apportion responsibility for these outcomes to organizational business units or individuals. Analysis of the cybersecurity outcomes in the Cybersecurity Framework core also can assist organizations in identifying common and hybrid controls and saving resources.

How the Digital Guardian Platform Can Help

- **Identify.** Digital Guardian empowers the security administration team and ensures units are held accountable for their respective functions. By organizing and classifying data, DG can facilitate the fact-based decisions required to support a successful cybersecurity framework and increase the clarity of the respective organization's risk profile.
- **Protect.** Digital Guardian identifies system level weaknesses to increase the understanding of cybersecurity vulnerabilities, while at the same time enforcing enterprise wide policy.
- **Detect.** DG adds key contextual information to correlative behavior allowing the security practitioners to make informed risk decisions.
- **Respond.** By understanding how data and systems are being used through reports shared among business units, organizations can make better informed security decisions and policies.
- **Recover.** DG's visibility not only shows data workflow and transactional movement, it can determine that disaster recovery protocols and processes are in accordance with component policy. DG's data enforcement and protection capabilities enhance an agency's recovery posture in support of managing an organization's cybersecurity program.

#6: Maintain A Comprehensive View of Cyber Risk

The Cybersecurity Framework Core can help organizations better organize their accepted risks and the risks they are working to remediate across all systems. This aggregate and comprehensive understanding of risk enables more informed and effective Risk Management Framework (RMF) authorization decisions.

How the Digital Guardian Platform Can Help

- **Identify.** Digital Guardian allows an agency to correlate gaps and vulnerabilities that are aggregated from Digital Guardian's endpoint agents and network sensors. Reporting and alerting can be triggered many ways including by user, groups, or machines. Reporting and analysis across groups of machines provides a comprehensive view to identify both specific and widespread issues.
- **Protect.** DG provides blocking of known and unknown threats. Blocking is accomplished based upon known threat behaviors, policy violations and detection of advanced threats.
- **Detect.** DG operates at both the endpoint and network for real time detection and policy enforcement. DG identifies data at rest risk exposure for all data repositories, including cloud services.
- **Respond.** DG provides alerting for real time notification to incident responders of active threats. Risk and severity can be assigned when data elements exposed by these risks are understood.
- **Recover.** DG provides the intelligence required for preparation in the event of a threat or a compromise, and maintains the integrity of the data, thereby reducing the level of effort and cost involved with remediation.

#7: Report Cybersecurity Risks

The Cybersecurity Framework Core provides a reporting structure and language that aligns to SP 800-53 controls. This alignment enables easy roll-up of control status into a reporting structure that is appropriate to and understandable by the appropriate stakeholders.

How the Digital Guardian Platform Can Help

- **Identify.** Digital Guardian is aligned with SP 800-53 controls and provides tactical and strategic level reporting for the analyst and security owner. DG provides comprehensive reporting and can also integrate with other third party reporting and analysis tools for a cohesive security framework. DG's configurable reporting tools allow maximum flexibility in sharing with other organizations.
- **Protect.** Understanding how data is accessed, used and shared is a key element to understanding risk. With the ability to see all activity around data usage, intelligent organizational policies based on how data is actually used can be developed with the business units.
- **Detect.** When used throughout tiered environments, DG identifies anomalistic and potentially malicious access to sensitive data and unauthorized processes.
- **Respond.** Accurate identification of cybersecurity risks and exposures through collective reporting allows incident management and forensic review. The incident response process often requires the participation of various specialists. DG's Analytics and Reporting Cloud (ARC) has workspaces that guide security professionals to the events that matter when identifying anomalous and suspicious insider and outsider activity. Analysts can easily drill down to follow an investigation and determine remediation steps.
- **Recover.** Industry best practices allow for recovery of user and system data and file access.

#8: Inform the Tailoring Process

Cybersecurity Framework Profiles enable organizations to reconcile mission objectives and cybersecurity requirements into the structure of the Cybersecurity Framework Core. This ability readily translates to the SP 800-53 controls that are most meaningful to the organization.

Profiles can be used to tailor initial SP 800-53 baselines into final baselines, as deployed in the RMF Implementation step.

How the Digital Guardian Platform Can Help

- **Identify.** Digital Guardian's strength is providing profiles of visibility and control policies that are aligned with any or all respective business and department units. Each agency has its own priorities and responsibilities and DG brings visibility into all risk elements and the prioritization of those elements for each organization. The DG solution provides flexibility and control organizations need to evolve to continuously changing security requirements. Administration of DG is based on roles and responsibilities and provides a separation of duty for individuals' respective authorization levels.
- **Protect.** DG capabilities enable organizations to facilitate implementation of security measures as defined in SP 800-53 and SP 800-37. This includes active enforcement of protections around insider and outsider threats, including securing users and systems operating outside of perimeter defenses.
- **Detect.** DG capabilities allow organizations to assess and rank data sensitivity, in order to focus their security program resources.
- **Respond.** Responses can be implemented based on the impact of an incident; low, medium or high, with additional granularity available. This capability assures the security practitioner that appropriate responses, flexible controls and relevant countermeasures are in place.
- **Recover.** By providing profiles which incorporate an understanding of normal behaviors and trends, as well as detailed forensic analysis of anomalies and violations, organizations can take a measured recovery approach, thereby optimizing resources.

Additional Resource

The NIST Cybersecurity Framework:
https://www.nist.gov/cyberframework

What is NIST SP 800-53? Definition and Tips for Compliance:
https://digitalguardian.com/blog/what-nist-sp-800-53-definition-and-tips-nist-sp-800-53-compliance

More information About Digital Guardian Federal Goverment Solutions:
https://digitalguardian.com/solutions/government

About Digital Guardian For Federal Organizations

Digital Guardian improves the ability of public-sector security pros to respond with certainty and effectiveness at the speed and scale of threat. Our offerings address the ongoing gap between the threats public organizations face, and the capabilities they need. Our single-agent approach protects sensitive data from both insider and outsider threats, across thousands of desktops and personal devices. And our solutions work with the major security platforms that public organizations already use, supporting a single pane of glass into data security.

Digital Guardian makes it easier to audit, monitor, and report on all end-user activity, regardless of device type; maintain and document compliance with Executive Order 13587; classify, categorize, and persistently tag organizational data; apply specific policy to documents which can prompt, block, and record user activity in real-time; and conduct investigative tasks like key logging, file capture, and screen capture.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.