Kiteworks

To: cyberframework@nist.gov
Atten: Kevin Stine, Cheri Pascoe

Kiteworks comments on
NIST CSWP 29 (Initial Public Draft) the NIST Cybersecurity Framework 2.0

Kiteworks appreciates the opportunity to provide feedback on the draft NIST Cybersecurity Framework (CSF) 2.0. As a leading cybersecurity company, Kiteworks technologies are used, and have been used to protect sensitive information and data across numerous industry sectors, including dozens of Federal Agencies, for decades.

Kiteworks has been a longstanding partner of the U.S. government and NIST and remains committed to partnering with NIST and the U.S. government to develop new best practices geared to protect the nation from emerging threats, including AI threats. We look forward to engaging with NIST as the draft evolves and remain available for any feedback.

We commend NIST for its continued leadership in developing and maintaining this important framework, which has helped organizations of all sizes to improve their cybersecurity posture. Overall, we believe that the CSF 2.0 draft is a significant improvement over the current framework. We are particularly pleased to see the focus on governance and automation, enabling further measurably of cybersecurity outcomes.

The NIST Cybersecurity Framework (CSF) 2.0 is a valuable resource for organizations of all sizes and industries. It provides a comprehensive and user-friendly way to explore the CSF Core. As NIST develops the CSF 2.0, use of the reference tool and tools like OSCAL to ensure mappings of controls will remain critical. Furthermore, Kiteworks is pleased to see that the CSF 2.0 Reference Tool is now available for public comment, as it has the potential to significantly improve the way organizations implement and manage the CSF and serve as a valuable asset to any cybersecurity-related organization. Nonetheless, we encourage NIST to continue to develop and improve the Reference Tool and to consider leveraging additional technology and automation tools.

- **Proposed additions of two additional prongs to the "Governance" pillar**

A robust cybersecurity framework must encompass effective technology management within an organization. As organizations continuously adopt and integrate new technologies, it is essential to establish a dedicated category focusing on the comprehensive management of these technologies. In the following section, a proposal for a new category, **Technology Management (GV.TM)**, was made aiming to scale the proposed governance controls by

introducing a clear and cohesive technology management strategy that can help mitigate these risks and protect the organization, while incorporating automated monitoring controls.

The technology management strategy should encompass aspects such as technology asset acquisition, deployment, maintenance, and decommissioning. Diverse technologies come with varying risk levels, including introducing potential vulnerabilities to the cybersecurity infrastructure. Therefore, a well-defined technology management strategy is vital to mitigate these risks and fortify organizational security. Furthermore, it is essential to include technology and automation tools to enhance the proposed governance framework ability to monitor risk at scale.

Like technology, data is also a critical asset often targeted in cybersecurity threats. Establishing a separate governance category for data management can significantly benefit the organization by covering strategies for secure data handling, storage, and disposal. This results in heightened protection for sensitive and business-critical data. Such strategy is key given the nature of AI threats vectors emerging to the introduction of generative AI solutions that interact namely with unstructured data and content, and need to align the CSF revisions with the development of new requirements under the released White House AI Executive order.

In the following section, a proposal for a new category, **Data Management (GV.DM**), was made to cover strategies for secure data handling, storage, and disposal, enhancing the safeguarding of sensitive and business-critical data. Given the multitude of existing data protection laws and regulations, such as GDPR and CCPA, and the enhanced focus on privacy and data governance given the rise of AI threats (e.g. the AI Executive Order), having a data management strategy becomes crucial. It ensures compliance with these emerging regulations, reducing the risk of legal complications. In the unfortunate event of a data breach, a pre-established data management strategy becomes instrumental as it expedites response times, aids in damage mitigation, and facilitates efficient recovery efforts, thereby enhancing overall cybersecurity resilience. Furthermore, data management controls can be introduced to align with the incorporation of new requirements for AI security and safety, such the expansion of NIST SSDF, the AI EO deliverables, and the AI RMF considerations, and take into account AI risk mitigation needs, as the CSF 2.0 evolves,

These capabilities can help organizations improve the efficiency and effectiveness of their cybersecurity programs, reduce the risk of human error, and improve their security posture while addressing emerging AI threat verticals stemming from the use of data. We encourage NIST to continue to develop these proposed pillars and provide guidance on how organizations can best implement these capabilities, while considering the introduction of automation and technology solutions to further enhance the governance function.

- CSF 2.0 Function GOVERN (GV)

1.1 Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)

The circumstances - mission, stakeholder expectations, and legal, regulatory, technological, and contractual requirements- surrounding the organization's cybersecurity risk management decisions are understood.

1.1.1 Ex2: Leverage technology to develop a process to track and manage legal and regulatory requirements regarding protection of individuals' data information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation) to reduce the risk of compliance violations and improve their overall data protection stance.

1.2 Subcategory GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated.

Establishing and implementing a suitable strategic assessment supported by technological controls to identify and quantify risks.

1.2.1 Ex2: Specify technology solutions leveraged to enforce and govern the criteria used to avoid data risk.

1.3 Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID.GV-02)

Cybersecurity roles, responsibilities, authorities and technology controls are used to foster accountability, performance assessment, capabilities and continuous improvement are established and communicated to enhance and scale the organization and its suppliers' risk management and governance.

1.3.2 Subcategory GV.RR-03: Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies

Implement adequate technological and other resources are allocated to commensurate with cybersecurity risk strategy, mechanism, roles and responsibilities, and policies.

1.3.3 Subcategory GV.RR-04: Cybersecurity is included in human resources practices (formerly PR.IP-11)

Develop cybersecurity human resources procedures to ensure cybersecurity is integrated and streamlined into practices.

Ex5: Implement a technology-enabled cybersecurity risk management policy and platform to integrate cybersecurity risk management considerations into all aspects of human resources processes.

1.4 Policies, Processes, and Procedures (GV.PO): Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced (formerly ID.GV-01).

Organizational cybersecurity policies, processes, and procedures, covering people, processes, and technology, as well as data access, handling, and sharing, are established, communicated, and enforced, guided by the tenets of the Zero Trust. (formerly ID.GV-1).

1.4.1 Subcategory GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced (formerly ID.GV-01)

-> Option 1: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities are communicated and enforced throughout the organization, leveraging suitable technology and cybersecurity capabilities to improve efficiency, effectiveness, and security.

-> Option 2: Policies, processes, and procedures for managing cybersecurity risks are established, carried out, and scaled using appropriate technology, based on organizational context, risk management strategy, and priorities. These are effectively communicated across the organization (formerly ID.GV-1).

Ex6: Communicate and develop a clear technology management strategy to mitigate risks, ensure regulatory compliance, and protect the organization's security and data.

1.4.2 Subcategory GV.PO-02: Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission (formerly ID.GV-01)

Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology proliferation, automated cybersecurity and organizational mission (formerly ID.GV-01)

Ex5: Implement technology and cybersecurity capabilities for managing cybersecurity risk management results and updating policies based on the results of periodic reviews.

1.5 Subcategory ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established (formerly RS.AN-05)

Risks associated with technology suppliers and their supplied products and services are identified, recorded, prioritized, and monitored (formerly ID.SC-2 and PR.DS-8)

1.6 Subcategory GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04)

-> Option 1: Suppliers and third-party partners are routinely assessed using audits, test results, or other evaluations to ensure compliance with contractual obligations and data protection under their custody.

-> Option 2: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. This includes ongoing tracking, control, and protection of data under their custody, leveraging technology solutions and enhanced controls.

-> Option 3: Implement third-party risk management, products, and services, to continuously monitor suppliers and third-party partners for cybersecurity risks and to automate the tracking, control, and protection of data in their hands.

1.7 Subcategory ID.SC-06: Supplier termination and transition processes include security considerations.

-> Option 1: Supplier termination and transition processes include specific security considerations, particularly focusing on the timely revocation of technology access and secure handling or transfer of data under their control.

-> Option 2: Supplier termination and transition processes include security considerations, and technology assessments focusing on response, transfer, and recovery planning.

- **Added additional sections:**

1. Category: Technology Management (GV.TM): Selecting and implementing technologies that meet the organization's security requirements to assess risks associated with new technologies.

   2.1 Subcategory

   GV.TM-1: Identifying and implementing a comprehensive technology management program to ensure that technology assets are acquired, deployed, maintained, and decommissioned in a secure manner, in support of the risk and governance program.

   Implementation Examples

   Ex1: Deploy technology security monitoring tools and systems to monitor risk-associated activity and improve security stance.

Ex2: Develop and implement a technology selection and procurement process to ensure that technologies meet the organization's security requirements, and increase compliance with relevant regulations and standards.

2. Category: Data Management (GV.DM): A comprehensive data protection program includes data handled, stored, and disposed of securely to enhance the organization's protection of sensitive and critical data.
   2.1 Subcategory
   GV.DM-1: Implementing appropriate security controls for data classification and management to ensure regulatory compliance and mitigate risks.
   Implementation Examples
   Ex1: A pre-established data management strategy, scaled by technology solutions, could speed up response times, mitigate damages, and help with recovery efforts.
   GV.DM-2: Conduct regular audits of the organization's data management practices to ensure compliance and security, supported by monitoring technology.
   Ex1: Develop a data inventory, supported by technology, to identify all data that is subject to data protection regulations.
   Ex2: Increase the efficiency and security of data management by implementing a data breach response plan.

Generally, across all CSF 2.0 controls, NIST should consider to recommend organizations to assess the suitability of technology controls and capabilities to enhance and scale the organization (and its suppliers') risk management and governance program.

Such a proposed control can be:

GV-TM: Assess the suitability of technology and cybersecurity capabilities to enhance and scale the organization and its suppliers' risk management and governance program.

- **Increase focus on data and unstructured content as an asset risk mapping and handling**

As explained above GV.OC-03, GV.RM-04, GV.SC-04, GV.SC-10 should explicitly cover, suggest, and indicate strategies for data handling, storage, and disposal, leading to enhanced protection of sensitive and business-critical data and outline paths to leverage technology in this regard. The mentioned subcategories should refer clearly and definitely to data protection by leveraging solutions such as asset tracking software, which helps monitor the location of assets containing sensitive data and manage the proper return or disposal of assets. Organizations can use software and other technology solutions to scan their systems for vulnerabilities that could violate data protection laws

or to track and report on employee access to sensitive data. Data encryption can also be used to protect data stored on assets during these processes.

    - **Risk Assessment and Risk Acceptance**: Organizations can use technology to assess and quantify risks associated with different types of data. This information is then used to establish risk acceptance criteria and implement risk avoidance strategies. For instance, encryption and multi-factor authentication can be employed to safeguard sensitive data.
    - **Supplier Management**: Technology assists in identifying and prioritizing suppliers based on their criticality to the organization. Supplier Relationship Management (SRM) software is used to track supplier information, assess supplier risk, and monitor supplier activity for suspicious behavior. This ensures that supplier-related risks are effectively managed.
    - **Asset Tracking and Data Protection**: Asset tracking software helps monitor the location of assets containing sensitive data. This information is vital for tracking and managing the proper return or disposal of assets. Additionally, data encryption can be used to protect data stored on assets during these processes.
    - **Supplier Termination and Data Leakage**: Technology aids in managing risks associated with supplier termination. Change management software can control changes to systems and data linked to supplier termination, while data backup and recovery solutions help restore systems and data in case of a breach. Data loss prevention (DLP) solutions and data encryption can also be employed to prevent unauthorized data transfers and protect sensitive data on supplier systems.
    - **Compliance Management**: Compliance management software automates the tracking and management of legal and regulatory requirements. It generates reports that help identify compliance gaps and develop remediation plans.
- Technology can help organizations to scale their understanding of risk and manage legal, regulatory, and contractual requirements regarding cybersecurity by providing tools to automate compliance monitoring and reporting. For example, organizations can use software to scan their systems for vulnerabilities that could violate data protection laws, or to track and report on employee access to sensitive data.
- Technology can also help organizations to respond to data protection incidents more quickly and effectively. For example, organizations can use cloud-based data loss prevention (DLP) solutions to automatically detect and block unauthorized transfers of sensitive data.
- Technology can help organizations to specify criteria for accepting and avoiding cybersecurity risks for various classifications of data. For example, organizations can use risk assessment tools to identify and quantify the risks to different types of data, and then use this information to develop risk acceptance criteria.

- Technology can also help organizations to implement risk avoidance strategies. For example, organizations can use encryption to protect sensitive data, or use multi-factor authentication to prevent unauthorized access to systems and data.

GV.SC-04 Control

- Technology can help organizations to know and prioritize their suppliers by criticality. For example, organizations can use supplier relationship management (SRM) software to track supplier information, assess supplier risk, and prioritize suppliers based on their criticality to the organization.
- Technology can also help organizations to monitor and manage supplier risk. For example, organizations can use security information and event management (SIEM) tools to monitor supplier activity for suspicious behavior or use vulnerability assessment tools to scan supplier systems for vulnerabilities.

GV.SC-10 Control

- Technology can help organizations to verify that assets containing their data are returned or properly disposed of in a timely, controlled, and safe manner. For example, organizations can use asset tracking software to track the location of assets or use data encryption to protect data that is stored on assets that are being returned or disposed of.
- Technology can also help organizations to mitigate risks to data and systems created by supplier termination. For example, organizations can use change management software to control changes to systems and data that are associated with supplier termination or use data backup and recovery solutions to restore systems and data in the event of a data breach.
- Technology can also help organizations to manage data leakage risks associated with supplier termination. For example, organizations can use data loss prevention (DLP) solutions to monitor and block unauthorized transfers of sensitive data, or use data encryption to protect sensitive data that is stored on supplier systems.

Overall, technology can play a significant role in helping organizations to protect their data and manage cybersecurity risks. By implementing appropriate technologies, organizations can reduce the likelihood and impact of data breaches, and comply with legal, regulatory, and contractual requirements.

Here are some proposed specific examples of how technology can help organizations to implement the above recommendations:

- GV.OC-03: Organizations can use compliance management software to automate the process of tracking and managing legal and regulatory requirements. This software can generate reports that help organizations to identify any gaps in their compliance program and to develop remediation plans.
- GV.RM-04: Organizations can use risk assessment tools to identify and quantify the risks to different types of data. This information can then be used to develop risk acceptance criteria and to implement risk avoidance strategies. For example, organizations may decide to encrypt all sensitive data, or to implement multi-factor authentication for access to critical systems.
- GV.SC-04: Organizations can use supplier relationship management (SRM) software to track supplier information, assess supplier risk, and prioritize suppliers based on their criticality to the organization. SRM software can also be used to monitor supplier activity for suspicious behavior.
- GV.SC-10: Organizations can use asset tracking software to track the location of assets that contain sensitive data. This software can also be used to generate reports that help organizations to identify assets that are at risk of being compromised. Organizations can also use data encryption to protect sensitive data that is stored on assets that are being returned or disposed of.

By implementing these and other technologies, organizations can significantly improve their data protection posture and reduce the risk of cybersecurity incidents. ***We look forward to discussing with NIST these proposals a the draft evolves, and remain available for any questions,***

Respectively,

Tim Freestone, CMO, Kiteworks