
December 13, 2013

Submitted via email to csfcomments@nist.gov

National Institute of Standards and Technology
Information Technology Laboratory
ATTN: Adam Sedgewick
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Re: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick:

The Financial Services Sector Coordinating Council[1] (FSSCC) appreciates the opportunity to provide comments in response to the National Institute of Standards and Technology Request for Comments on the Preliminary Cybersecurity Framework ("Framework").

FSSCC submits this response to demonstrate the deep commitment of the financial services sector to the public-private partnership envisioned by the Framework. We recognize that developing a Framework that applies to those critical infrastructure institutions in each sector requires a comprehensive discussion. We commend NIST for establishing a process that allows the private sector to provide input into developing the Framework. Each sector relies heavily on others for business functions. We must all work together to better secure our nation's infrastructure.

**Risk-Based Approach**

Overall, the FSSCC supports the Framework's use of a Capability Maturity Model Integration (CMMI) to encourage entities with critical infrastructure to analyze their current level of maturity and then work toward their next level of maturity using a gap analysis. This will enable entities of all maturity levels to leverage the Framework to strengthen their cybersecurity programs by establishing a guide for companies to assess and continuously improve their internal cybersecurity posture. This flexible and mature approach will both strengthen their cybersecurity program and align with business objectives.

Institutions with critical infrastructure must be able to implement the Framework in a risk-based, flexible, and cost-effective manner to accommodate differences across sectors, as well as differences within each sector that adopts this voluntary framework. The FSSCC believes that, as intended, an organization can reduce its risk by adopting the Framework. However, senior leadership will need to be engaged in order to make decisions on where to increase their level of investment in either budgetary outlays or human capital. It is, therefore, essential that the Framework

[1] A description of the FSSCC and membership list is available in Attachment A.

emphasize the need for companies to use the Framework to analyze what is truly at risk and what threats are most applicable to them and have the flexibility for companies to make the decision on where to prioritize precious capital to mitigate those risks and threats.

The Framework should be able to align with and reflect an organization's governance of cybersecurity risk, including the organization's existing risk assessment and risk management processes. This can enable widespread adoption by organizations, limiting duplication of efforts. For organizations that are less mature in their cybersecurity risk management efforts, the Framework should provide a starting point to build a cybersecurity risk management program.

The Financial Sector believes that, regarding Framework implementation, government should evaluate a BETA Test protocol to assess the efficacy of the Framework, identify meaningful deficiencies in implementation that reduce the effectiveness of the Framework, and provide key recommendations for improvement. Such a protocol should include a broad cross-section of sectors and companies that are representative of the wide variety of businesses for which the Framework is intended.

**Privacy and Cybersecurity**

Financial sector companies are accustomed to and are strongly supportive of protecting their customers' data and, as partners and service providers, the data of customers of financial institutions worldwide. The financial sector is currently subject to stringent laws and regulation that require them to protect the confidentiality as well as the security of their customers' nonpublic personally identifiable information, including the Gramm-Leach-Bliley Act ("GLBA"), the Fair Credit Reporting Act ("FCRA") and the Right to Financial Privacy Act. These laws and regulations are reinforced by regular, pro-active review and audit by highly specialized regulators.

However, the FSSCC believes that critical to successful adoption and implementation of this Framework is a clear risk-based methodology that strengthens cybersecurity programs, appropriately highlights privacy considerations, takes into account existing requirements, and supports continued innovation and effective business management strategies, regardless of sector. Therefore, FSSCC offers the following recommendations regarding the cybersecurity and privacy methodologies presented by the Framework.

Foundationally, the Framework should guide implementing companies to consider network security interactions as it relates to privacy. However, as written, the privacy methodology outlined by Preliminary Cybersecurity Framework Appendix B is likely to conflict with confidentiality and security requirements to which financial institutions are subject. As a result, as currently proposed, the Framework could have the opposite effect from that intended, resulting in less private sector usage of the voluntary Framework. We agree with the importance of privacy protections within the Framework. However, privacy should be integrated in the Framework without impacting Framework adoption by redefining key aspects of network security and privacy. In addition, we must recognize the need for a necessary balance between privacy and security to ensure institutions can still protect themselves from malicious actors.

The Framework's discussion must focus on the privacy issues that are uniquely impacted by an organization's cybersecurity measures or compensating controls. Not all cybersecurity activities, measures or controls have privacy implications. The Framework's choice of a definition of personally-identifiable information (PII) and a number of the specific elements of the proposed methodology runs counter to the stringent laws and regulations with which the Financial Sector already complies to protect nonpublic personally identifiable information, including the GLBA, the FCRA and the Right to Financial Privacy Act. The Financial Sector by any measure is very mature when it comes to balancing cybersecurity with privacy. Its rules and regulatory model work. The Framework needs to take

this into account and allow for sectors that have a well established regulatory schema in place to adopt the Framework without running counter to those existing regulations. Any privacy discussion must clearly recognize the existing laws and regulations in this space similar to the recognition given in the Framework Core.

We believe the Framework's privacy methodology should not include civil liberties as it is the responsibility of Congress to create laws to protect civil liberties and institutions implement subsequent requirements. We believe that this is the intended relationship between civil liberties and private industry. In order for institutions to adopt the Framework, it will be essential that additional liability risks not be introduced by the inclusion of civil liberties.

To address these concerns, the sector supports the "Alternative Methodology to Protect Privacy for a Cybersecurity Program" as provided to NIST on December 5 by Harriet Pearson, Partner of Hogan Lovells, and noted in Attachment B.

**Future Framework Efforts**

Overall, we believe issues relating to the future roadmap should be addressed outside of the Framework document. This will allow the Framework to be succinct and focused for practitioners to implement within their systems.

The Preliminary Cybersecurity Framework provides a comprehensive list of Areas for Improvement in Appendix C. NIST can be a true leader for protecting cybersecurity by coordinating efforts on future workforce development and supply chain risk management. We agree with the recognition by NIST for the need to improve the sharing of threat indicators. However, Congressional action addressing legal liability protection for the sharing of cyber threat information across sectors must be fully addressed. Further, sharing of additional threat information will enable institutions to adequately and properly prepare their Framework self-assessments.

We agree with NIST's assessment that the Framework must be continuously evaluated and updated. However, the update should not occur until the first version has been adopted and an assessment has been completed to evaluate the challenges experienced during the adoption. We believe the critical infrastructure community must be involved in this effort and the public-private partnership is uniquely situated to provide the necessary participation. The future of the Framework should leverage the existing sector coordinating councils to ensure adequate participation of all sectors.

**Conclusion**

The FSSCC applauds NIST's engagement with the private sector in developing the Framework and we look forward to continuing these efforts moving forward. Only with substantive and significant engagement with the private sector will the voluntary Cybersecurity Framework achieve its goals to improve the security of critical infrastructure.

Respectfully submitted,

Charles Blauner
Chair
Financial Services Sector Coordinating Council (FSSCC)

**Attachment A: Financial Services Sector Coordinating Council (FSSCC) Membership**

The Financial Services Sector Coordinating Council (FSSCC) fosters and facilitates financial services sector-wide activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The Council was created in June 2002 by the private sector, with recognition from the U.S. Treasury, to coordinate critical infrastructure and homeland security activities in the financial services industry.

| Associations | Operators | Utilities and Exchanges |
|---|---|---|
| American Bankers Association (ABA) | Aetna | BATS Exchange |
| American Council Life Insurers (ACLI) | American Express | CLS Services |
| American Insurance Association (AIA) | Bank of America | CME Group |
| American Society for Industrial Security International (ASIS) | BNY Mellon | Depository Trust & Clearing Corporation (DTCC) |
| Bank Administration Institute (BAI) | Citi | Direct Edge |
| BITS/Financial Services Roundtable | Equifax | First Data |
| ChicagoFIRST | Fannie Mae | Intercontinental Exchange (ICE) |
| Consumer Bankers Associations (CBA) | Fidelity Investments | International Securities Exchange (ISE) |
| Credit Union National Association (CUNA) | Freddie Mac | LCH Clearnet |
| Financial Information Forum (FIF) | GE Capital | NASDAQ |
| Financial Services Information Sharing and Analysis Center (FS-ISAC) | Goldman Sachs | National Stock Exchange |
| Futures Industry Association (FIA) | JP Morgan Chase | NYSE Euronext |
| Independent Community Bankers Association (ICBA) | MasterCard | Omgeo |
| Investment Company Institute (ICI) | Morgan Stanley | Options Clearing Corporation |
| Managed Funds Association (MFA) | Navy Federal | The Clearing House |
| National Automated Clearing House Association (NACHA) | Northern Trust | |
| National Association of Federal Credit Unions (NAFCU) | PNC | |
| National Armored Car Association (NACA) | RBS | |
| National Futures Association (NFA) | Sallie Mae | |
| Securities Industry and Financial Markets Association (SIFMA) | State Farm | |
| | State Street | |
| | Sun Trust | |
| | US Bank | |
| | Visa | |
| | Wells Fargo | |

**Attachment B: Methodology to Protect Privacy for a Cybersecurity Program**

This part of the Cybersecurity Framework presents a methodology to address the collection and use of protected information related to an organization's cybersecurity activities. This part does not extend or apply to commercial data activities outside of the cybersecurity context.

Securing personal information is an element of both cybersecurity as well as privacy programs overall, and is addressed in Appendix A (Framework Core) in a number of relevant categories such as Risk Assessment (RA), Risk Management Strategy (RM), Data Security (DS), Information Protection Processes and Procedures (IP), and Protective Technology (PT). Securing such information is therefore not addressed in this part.

The term "protected information" used in this part means "personal information that (i) is subject to security breach notification requirements, (ii) an organization is restricted by law from disclosing, (iii) an organization is required by law to secure against unauthorized access, or (iv) an organization voluntarily so designates."

| Potential Privacy Considerations Related to Cybersecurity Activities | Organizational Privacy Measures and Controls |
|---|---|
| An organization's overall governance of cybersecurity risk should consider privacy implications of its cybersecurity program. | An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program.<br><br>Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained.<br><br>Process is in place to support compliance of cybersecurity activities with applicable privacy laws.<br><br>Process is in place to assess implementation of the foregoing organizational measures and controls. |
| Approaches to identifying and authorizing individuals to access organizational assets and systems may raise privacy considerations. | Steps are taken to identify and address the privacy implications of access control measures to the extent that they involve collection or use of protected information relating to identifiable individuals. |
| An organization's cybersecurity monitoring activities may raise privacy considerations. | Process is in place to conduct a privacy review of an organization's cybersecurity monitoring activities |
| Information-sharing pursuant to cybersecurity activities may raise privacy considerations. | Process is in place to assess and address whether, when, how, and the extent to which protected information is shared outside the organization as part of cybersecurity information sharing activities. |
| The organization's cybersecurity awareness and training measures should include privacy considerations. | Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities.<br><br>Service providers that provide cybersecurity-related services for the organization are informed about the organization's applicable privacy policies. |