Apr 25, 2022

Katie McFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comments of Salesforce, Inc.

Salesforce, Inc. ("we," "us," "SFDC," or "Salesforce") appreciates the opportunity to respond to the National Institute of Standards and Technology's ("NIST") Request for Information ("RFI") to evaluate and improve the NIST Cybersecurity Framework and Cybersecurity Supply Chain Risk Management resources.

About Salesforce

Salesforce is a global leader in cloud enterprise software for customer relationship management (CRM), providing software-as-a-service ("SaaS") and platform-as-a-service ("PaaS") offerings to businesses. Founded in 1999, Salesforce provides business-focused software to businesses, governments and other organizations around the world. We operate globally in the business-to-business (B2B) environment, and our customers represent companies of all sizes and across all sectors. Our business model is cloud-based and low code, allowing for faster deployment of technologies and greater agility. We help our customers connect with their customers — or employees or citizens — in a whole new way using cloud, social and mobile technologies.

Trust and security are built into everything we do: from one strong security team (more than 1,700 cybersecurity professionals and growing) working across all clouds, to common security controls across all platforms. Our engineers build defense-in-depth into our systems— which is another way of saying we try to prevent a single-point-of-failure through our security tools, processes and approaches to prevent, detect and respond to any security threat.

Salesforce & Cybersecurity

Our customers are entities who want to build stronger relationships with their customers and other stakeholders. As a result, customers trust us with some of their most sensitive data, making the protection of that data fundamental to our ability to serve our customers. It is important for us to focus on business and engineering agility and we believe security is an enabler for innovation. It is why we have implemented a comprehensive privacy and security program, which includes achieving the authority to operate certain services authorized against the FedRAMP High Impact Level and DoD Impact Level 4 baselines, and obtaining key certifications such as ISO 27001/17/18.

Our engineers build defense-in-depth into our systems because we know that taking a risk-based approach is critical to maintaining world-class security. In addition to our more than 1,700 security professionals we also have dozens of security tools, processes and approaches to prevent, detect and respond to security threats. Across our entire organization, we utilize the NIST CSF. This metrics-based framework enables Salesforce to measure our security effort and project by tying it back to the five pillars of NIST CSF (Identify, Protect, Detect, Respond, Recover). Our risk-management program maps our security initiatives to the risks that they are meant to address. Some of the key areas of the program include risk assessments and reporting, including the risks posed by third-party products (3PP), product infrastructure, and the supply chain. We conduct an annual security risk assessment on security risk areas across the company.

We have customers from around the world spanning dozens of sectors and industry verticals. We work closely with them to ensure that our data protection programs meet their diverse business and regulatory needs and requirements. This breadth and depth of experience gives us unique insights into approaches to cybersecurity that work—and we in turn share that information with our customers large and small. Salesforce believes that CSF is a top priority; as a result, we offer the following additional specific insights and recommendations:

Usefulness of the NIST Cybersecurity Framework

Salesforce maintains a formal Company-wide information security management system (ISMS) that conforms to the requirements of the ISO 27001 standard, FedRAMP, DoD cloud computing authorization, and the NIST CSF, including security policies, standards, and procedures. Salesforce works to integrate security requirements into the business and ensure control effectiveness is measured and reported, enabling risk informed decisions that support business objectives.

In particular, our Security Governance, Risk Management, and Compliance (GRC) team uses the CSF as a security capability maturity model. These teams identify and monitor associated initiatives and perform impact analyses on an ongoing basis. Further, Salesforce engages an external, independent third party to calibrate Salesforce's CSF maturity ratings at an enterprise and business unit level. The insights from these teams allow for SFDC leadership along with security capability owners to review and utilize recommendations from the assessments to identify where opportunities exist to uplift maturity in their respective areas.

Salesforce has found that the NIST CSF complements our existing cybersecurity strategy and while it is just one of many frameworks available to draw on, combined with other controls, it allows us to evaluate our overall security maturity. We believe that outputs of the CSF maturity assessment are most useful when utilized in conjunction with internal security risk assessment results. The two sources are considered independently and combined to inform security strategy and optimize investment decisions to both reduce security risk and increase maturity.

Proposed Changes to the CSF

CSF Tiering Details. Currently, Salesforce services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis. To enhance objectivity and the ability to re-perform maturity assessments across assessors internal and external, it would be helpful to add detail on requirements for each tier. This should include additional guidance on building out profiles, profile templates, detailed level references leveraging specific mappings to other standards and frameworks (e.g., NIST 800-53, ISO 27x). This would add a layer of maturity guidance to the existing design guidance inherited through the mappings.

Interoperability. Globally, there has been a proliferation of security frameworks, and the US is no different. Beyond the CSF, there are several layers of guidance and frameworks that are built

upon one foundation but are not simplified into one clear standard. Salesforce would support enhanced, clear and simplified interoperability between the CSF and risk management frameworks (e.g., NIST RMF/800-37, NISTIR 8286, ISO 31000) and control standards (e.g., NIST 800-53, ISO 27x). While Salesforce does have the resources to sort through the different frameworks, tying the concepts of risk, control effectiveness, control maturity and control design together would be helpful and drive efficiency in security programs in both large and smaller companies.

- Accessibility. The promotion of interoperability will also promote accessibility. The supply chains of companies are often made of companies of varying sizes and capabilities, therefore it is critical for guidance to be accessible and clear so that smaller companies can leverage this content to improve their private and security capabilities. Absent this accessibility, many larger companies could be impacted through supply chain relationships.

Cloud Addendum. The Federal government has several schemes which were established to provide a standard, centralized approach to assessing and authorizing cloud computing services and products for the entire US Federal Government. These schemes are required to comply with FISMA. The NIST RMF was created to provide a consistent approach to supporting FISMA requirements. The schemes are closely related to and based off of the NIST CSF. Two such examples are the FedRAMP and DoD cloud computing authorization processes, which are interpretations of the NIST RMF applicable to cloud service providers. Salesforce believes that this RFI, presents an opportunity for NIST to create a cloud addendum that aligns and map the CSF to the cloud computing baselines and authorization processes.

Use of non-NIST frameworks

Salesforce believes that cybersecurity frameworks can be both effective and voluntary when the scheme is crafted to comport with existing international standards and not create additional and divergent security practices.

Global entities face a plethora of security risk, maturity and control frameworks and regulation each with their own intrinsic value. There are many commonalities amongst them. Most entities must manage the commonalities and differences via vendor support and/or internal resources continuously monitoring the external landscape and managing internal common control frameworks. The level of effort to execute and maintain mappings across the various global security regimes is nontrivial. When such activities are performed by multiple independent teams, or different companies across the supply chain, the results themselves are not uniform.

Salesforce would urge NIST to consider the publishing of authoritative and official interoperability supporting tools and data sets, with the aim of providing some assurance around international interoperability with other global certification schemes. We appreciate NIST's efforts around OSCAL (Open Security Controls Assessment Language), which can be used to represent compliance frameworks in a machine-readable way. Salesforce believes that this work could form a foundation for representing other industry compliance frameworks in a more standardized way. To be clear, the varying controls would still need to be mapped to one another, but the data formatting and interchange problems could potentially be addressed. We believe this would provide clarity and enable optimized resource utilization.

Gaps in Existing Cybersecurity Supply Chain Risk Management Guidance and Resources

Salesforce uses third-party service providers, including software and hardware vendors to ensure reliable services to our customers. As we've seen globally over the past year, there has been an increase in supply chain-related attacks using third-party services providers as an attack vector. As such, there is an opportunity to continue to expand guidance produced by NIST to cover emerging risks facing security teams, with supply chain risk management being a key area.

Salesforce recognizes that work has and continues to be done to provide tools and mapping to address the maturity of security programs in this emerging area. We would request NIST to continue to focus on this emerging risk with an eye toward new threats and attack types.

Conclusion

As a company, Salesforce is proud of our collaboration in the industry to invest in the necessary tools, training and support for our customers and employees. We understand that as the cloud and other new forms of technology emerge, the potential risk profiles increase.

We truly believe in the urgent need to continue to work toward a global response to address systemic cybersecurity challenges and improve digital trust, to defend innovation and protect institutions, businesses, and individuals. As such, we appreciate NIST's efforts to evolve with the changing landscape.

Respectfully,
Vikram Rao
Chief Trust Officer