Doing business securely in the financial services industry

JPMorgan Chase Summary of Guidance from the U.S. Treasury and industry regarding key security and risk management practices for new suppliers seeking to serve financial services industry

February 2019

Preface

The financial sector is a critical part of the U.S. economy. Advancing the **safety, soundness, and resiliency of the financial sector** by mitigating and protecting it from risks is a **shared goal** for all financial sector participants as well as financial services regulatory community.

Companies that seek to do business in the financial sector as **suppliers are required to perform all their activities in a safe and sound manner and in compliance with applicable laws.** This is especially important when a supplier service involves access to confidential data or delivery of critical service.

Currently there are numerous regulatory and industry sources that specify such requirements. New suppliers are finding it difficult to comprehend and comply. This situation creates a barrier to entry that could stifle innovation and reduce competitiveness.

The U.S. Treasury Guidance helps to consolidate existing requirements into a **clear, concise set of nationwide best practices that new suppliers seeking to serve financial sector should adopt and be ready to demonstrate.**

- The Guidance was developed in early 2018 by the U.S. Treasury and representatives of several U.S. financial institutions.
- The Guidance is organized around the five categories of the NIST Cybersecurity Framework[1], with "Engage" category added to cover requirements beyond cybersecurity (for example, financial stability requirement for new suppliers).

The U.S. Treasury encourages all companies that are positioning themselves to become suppliers to the financial sector to consider and adopt this Guidance. This will enable such companies to effectively engage with financial institutions, and also elevate the security of new suppliers' operations–thus helping to keep our industry and our country safe.

1 National institute of Standards and Technology Cybersecurity Framework (NIST CSF) is the de facto standard for firms seeking guidance to counter cyber threats according to U.S. Department of the Treasury, Office of Financial Research, "Financial Stability Report" of 15th December 2017. Federal entities and Sector-specific agencies (SSA) are promoting and supporting the adoption of the NIST CFA in all critical infrastructure sectors (including financial sector).

Key security and risk management practices for new suppliers seeking to serve financial services industry

Identify

1. Supplier should **identify, classify and manage all assets**–data, systems, software, devices, personnel, facilities, any other–that it uses to provide services to financial institutions.
2. Supplier should establish a **risk management program** to proactively identify, assess and mitigate risks to all assets that it uses to provide services to financial institutions.
3. Supplier should establish a **third party risk management program** to proactively manage risks associated with their third parties and subcontractors.
4. Supplier should establish policies, procedures, controls to ensure **compliance** with all applicable legal, regulatory, risk, security and operational requirements.

Protect

5. Supplier should implement **perimeter and network security** controls to permit only approved and authorized communications between network domains.
6. Supplier should **limit access** to data, systems, software, devices, personnel, facilities and other to only authorized users to perform authorized activities.
7. Supplier should **encrypt data** while in transit and at rest and have implement adequate measures to manage and protect cryptographic keys.
8. Supplier should **protect data throughout data lifecycle** (from creation through disposal), consistent with supplier's risk management strategy.
9. Supplier should ensure that all systems are **configured securely,** and review security configurations on a regular basis.
10. Supplier that develops software should implement **secure software development practices.**
11. Supplier should have strict **change management** procedures that require documentation, review and approval of all changes to production environment.
12. Supplier should provide regular **training and communications** on security policies and risks such as social engineering, phishing and other.
13. Supplier should have **standard contract terms** for their third parties. The terms should include all relevant legal protections.

Key security and risk management practices for new suppliers seeking to serve financial services industry (cont'd)

Detect

14. Supplier should continuously gather and analyze information on new and existing **threats and vulnerabilities.**
15. Supplier should enable logs of key systems and user activities, and on a regular basis **aggregate and analyze logs** to identify any unauthorized activity.
16. Supplier should periodically **scan internal and external networks and applications** for vulnerabilities.
17. Supplier should implement **Data Loss Prevention** mechanisms to limit unauthorized or unintentional exfiltration of data.
18. Supplier should implement a **background check** process for its employees and contractors.

Respond

19. Supplier should have an **incident response** plan. Staff should be trained to execute the plan and execution should be tested periodically. Incident response plan should include notification to affected financial institutions.
20. Supplier should implement a strict **patch management** process to identify and classify vulnerabilities, and implement patches within a defined and reasonable timeframe.

Recover

21. Supplier should maintain **business continuity and disaster recovery** plans that define resources and actions to help minimize losses in the event of a disruption to the business unit, application, or infrastructure.
22. Supplier should periodically **backup data** in a secure manner and verify recoverability of data and software.

Engage

23. Supplier should be able to provide audited financial statements to demonstrate their **financial stability** to financial institutions they are looking to engage with.
24. Supplier should **support assessments of its controls** by the financial institutions and assessment firms. This includes providing the required controls documentation, as well as allowing assessors to inspect and test controls.