CISCO - SUPPLY CHAIN RISK MANAGEMENT PROJECT MANAGEMENT PLAN

Version *1.0*
12/10/2022

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE OF PROJECT MANAGEMENT PLAN

This project management plan (PMP) lays out the steps needed to improve Cisco C-SCRM posture by transitioning to the manufacturing of critical infrastructure equipment in a US-based domestic partner's facility. The PMP details the standards and practices the domestic partner will be held to. The intended audience of the Cisco Networking Critical Infrastructure Supply Chain Risk Management Plan is all project stakeholders, including the project sponsor, senior leadership, and the project team. This PMP outlines the problem that will be addressed, the work that will be completed as part of the project, the schedule and budget the project will follow, and the management of quality, human resources, communications, risks, and procurement. This project is a small-scale test focused on supporting a third-party manufacturer’s new router manufacturing site to meet the following cyber-SCRM objectives outlined in Executive Order (E.O.) 14017 and E.O. 14088.

2 EXECUTIVE SUMMARY OF PROJECT CHARTER

2.1 INTRODUCTION

The production of US critical infrastructure and supply chain resilience are deeply important to Cisco. Overseas manufacturing of such equipment possesses inherent drawbacks that only domestic manufacturing can overcome. Our team aims to improve our C-SCRM posture by manufacturing critical infrastructure equipment in a US-based facility. Partnering with Cisco, the domestic manufacturer will be held to Federal and CISA directives and implement the most up-to-date cybersecurity practices. Quality will be monitored using Highly Accelerated Lifecycle Testing (HALT) and Real-time data AQ strategies.

2.2 COMPANY ROLE

Cisco will develop a set of processes and guidelines for manufacturers to meet to create critical infrastructure-related products for Cisco. If the pilot outlined in this PMP is successful and yields profitable results for Cisco, the target state will be to implement the controls defined for this project on all contracting parties and manufacturers. Furthermore, Cisco will act as a consultant for the US-based contracting party in the pilot to advise them on controls and security measures that must be implemented.

2.3 PROBLEM

US critical infrastructure support and supply chain resilience is paramount at Cisco. Overseas manufacturing of US critical infrastructure equipment possesses inherent drawbacks that only domestic manufacturing can overcome. China sponsors Advance Persistent Groups (APT) groups to collect intelligence and craft threat vectors, and perform attacks on US interests. All of Cisco's manufacturing is located in China, and with that being our near-peer adversary, it is critical that we move to a domestic production model for Critical Infrastructure. With the increase in Zero-Day attacks stemming from China, we cannot risk our cyber resilience for short-term economic gain. Additionally, China has been unable to meet production agreements based on an unstable workforce resulting in a multi-billion dollar backlog. As China cannot sustain an active force while they are in our good graces, it is hard to predict their reliability in a state of conflict.

2.4 SOLUTION

To transition Cisco’s critical infrastructure equipment domestically, the following objectives are proposed: Project Team will enable the successful transition from the foreign

manufacturers in China to the new domestic sites. The new domestic partner will take full responsibility for production and cease production of Cisco's critical infrastructure production line in China. Domestic manufacturers will maintain a registry of all software and hardware systems. The new manufacturer will have an account of all supplier SBOM/HBOM meeting the Dept. of Commerce's published minimum elements. Lastly, the manufacturer ensures cyber security best practices when manufacturing, patching, and upgrading Cisco's products.

2.5 JUSTIFICATION

Cisco is a critical component for many US-based organizations for their networking. As such, supply chain management is becoming increasingly important. As most of Cisco's hardware suppliers are located in China, this presents a risk to the Company as national regulations such as Executive Orders 14017 and 14088 become stricter on using offshore contractors.

Moving towards using US-based manufacturers will allow Cisco to sell to the US government and associated organizations.

2.6 CONCLUSION

Cisco is a frontrunner when it comes to producing critical infrastructure for both the US government and private entities. Continuing production in a country that is becoming exceedingly more of a cyber threat, along with allowing a growing backlog of work, is an issue that must be handled. Maintaining critical infrastructure production in China will only lead to further Zero-Day attacks and hurt the reputation of the organization as a whole. By implementing the process detailed in this project plan, we will drive necessary change and avoid the aforementioned associated risks of foreign critical infrastructure production.

2.7 OBJECTIVES

This project is a small-scale test focused on supporting a third-party manufacturer's new router manufacturing site to meet the following cyber-SCRM objectives outlined in Executive Order (E.O.) 14017 and E.O. 14088. The project team will (1) establish systems to account for the manufacturer's entire network infrastructure; (2) establish systems to collect and prepare the manufacturer's Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM); (3) identify, assess, and plan for mitigation of critical known vulnerabilities within the manufacturer systems; (4) prepare and test systems for mass-patching across all infrastructure.

2.8 ASSUMPTIONS & CONSTRAINTS

Assumptions:

- Foreign production will continue until domestic production is ready.
- Following the timeline, Cisco will terminate production/contracts on the 91st day of the project.
- In case of timeline setbacks, Cisco has allotted for extending the timeline for project work, including overseas production continuation.
- Domestic vendors will adhere to the set standards of production of critical infrastructure hardware.

Constraints:

- Budget
- Unforeseen risks/setbacks
- Time (extra time budgeted)
- Relationships with vendors

3 SCOPE MANAGEMENT

Cisco Networking Critical Infrastructure Supply Chain Risk Management (CNCISCR) will establish systems for the manufacturer's entire network infrastructure. The project aims to develop strategies to collect and prepare the manufacturer's Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM). The project plan will be applicable to the CNCISCR overseeing council, Cisco management team, Cisco engineering team, and business partnership under a legal contract with Cisco. The project will also identify, assess, and plan to mitigate known critical vulnerabilities within the manufacturer systems; prepare and test methods for mass-patching across all infrastructure. Cisco aims to deliver the project in three months, starting from January 1st, 2023, to April 1st, 2023, with a projected budget of one million United State Dollars.

3.1 STAKEHOLDER RELATIONS

3.1.1 Cisco Networking Critical Infrastructure Supply Chain Risk Management Roles

The project stakeholders consist of Project Champion, Project Sponsor, Project Management Team, and Project Team.

3.1.2 Project Champion

Vice President of Engineering Sundar is the project champion, where he ensures everyone is on board and on track to complete the project successfully and on time. Project champions promote continuous improvement initiatives throughout the organization and advocate for the project to ensure stakeholders are satisfied.

3.1.3 Project Sponsor

Senior Director of Software Development Jonathan Davidson is the project sponsor who provides resources, support, and leadership to the project team. He will act as a link between the project manager and other decision-making groups.

3.1.4 Project Management Team

Director of Manufacturing and Supply Chain Elon Sumk and Cybersecurity Supply Chain Risk Manager Jon Boyens are part of the project management team. They are leading members in planning, executing, monitoring, controlling, and closing out projects.

3.1.5 Project Team

The Security Engineering and Risk Management team, including Technical Lead Software Development Angela Smith, Senior Cyber Risk Analyst Huong Trinh, Product Security Architect Dr. Ron Ross, Senior Corporate Counsel – Data Security Practice John G. Roberts Jr, and Senior Financial Analyst Scott Liang are a team member of the project. They contribute to overall project objectives, offering expertise to achieve predetermined goals. They will work in a team and collaborate to meet business needs.

3.2 WORK BREAKDOWN STRUCTURE

Cisco Networking Critical Infrastructure Supply Chain Risk Management Work Breakdown Structure

3.2.1 Supply Chain Risk Management Project management

3.2.1.a Security Engineering and Risk Management Planning

3.2.1.b Supply Chain Risk Management Planning

3.2.1.c Manufacturing and Supply Chain Management Meeting

3.2.1.d Cisco Supply Chain Risk Management Administrative Meeting

3.2.2 Supply Chain Risk Management Product Requirements

3.2.2.a Software Requirements for Supply Chain Risk Requirements

3.2.2.b Hardware Requirements for Supply Chain Risk Requirements

3.2.2.c Product Requirements Documentation

3.2.2.d Training Program Materials

3.2.3 Supply Chain Risk Management Detail Design

3.2.3.a Software for Supply Chain Risk Detail Design

3.2.3.b Hardware for Supply Chain Risk Detail Design

3.2.3.c Product Detail Design Documentation

3.2.3.d Training Program Materials

3.2.4 Networking Critical Infrastructure Supply Chain Risk Construction

3.2.4.a Software for Supply Chain Risk Construction

3.2.4.b Hardware for Supply Chain Risk Construction

3.2.4.c Product Construction Documentation

3.2.4.d Training Program Material

3.2.5 Networking Critical Infrastructure Supply Chain Risk Integration and Testing

3.2.5a Software for Supply Chain Risk Integration and Testing

3.2.5b Hardware for Supply Chain Risk Integration and Testing

3.2.5c Product Integration and Testing Documentation

3.2.5d Training Program Materials

3.3 DEPLOYMENT PLAN

3.3.1 Cisco Release Considerations

3.2.1.a Timing of release

Project will be released on 4/01/2023.

The Supply Chain Risk Management Project management phase is from

01/01/2023 to 01/26/2023.

The Supply Chain Risk Management Detail Design phase is from 01/27/23 to 02/24/23.

The Supply Chain Risk Management Detail Design phase is from 02/27/2023 to 03/10/2023.

The Networking Critical Infrastructure Supply Chain Risk Construction phase is from 03/13/2023 to 03/24/2023.

The Networking Critical Infrastructure Supply Chain Risk Integration and Testing are from 03/27/23 to 04/01/23.

3.2.1.b Budgeting

The project will have a budget of one million dollars.

3.3.3 Training

Members involved in the Cisco Networking Critical Infrastructure Supply Chain Risk Management project will conduct training through a web conference for one week using the company's devices. The budget for the training is part of the project budget. The training will occur throughout the entire project.

3.3.4 Accountability for deployment plan

Project Champion - Vice President of Engineering Sundar Agrawal has finalized changes and enhancements to the system throughout the entire project.

Project Sponsor - Senior Director of Software Development Jonathan Davidson owns the data and authorizes changes during software development updates.

Project Management - Director of Manufacturing and Supply Chain Elon Sumk and Cybersecurity Supply Chain Risk Manager Jon Boyens is responsible for input and retrieval protocols, retention standards, and security responsibilities.

Team Members - Technical Lead of the Software Development Department Angela Smith and her team are responsible for undertaking, and analyzing briefs, writing progress reports, identifying technical risks, and developing effective solutions following the project software requirements.

Team Member - Senior Corporate Counsel Data Security Practice John G. Roberts Jr. will provide global escalation and subject matter expertise support to Cisco contract negotiators for data security, data protection, and supply chain risk management terms in customer-facing commercial contracts.

Team Member – Senior Financial Analyst Scott Liang will drive financial forecasting, operating financial analysis, and oversight the network critical infrastructure supply chain risk management financial performance.

3.4 CHANGE CONTROL MANAGEMENT

3.4.1 Change Control Process Approach

Cisco will allow change requests on projects in many forms, such as oral, written, formal, or informal. The project Manager will document any changes that happen during

the project to avoid any potential problems. Significant changes submitted to the project champion will be formally reviewed and analyzed to determine their appropriation.

3.4.2 Change Control Process Structure

The change control process involves five steps; initiation, assessment, analysis, implementation, and closure.

3.4.3 Change Request Initiation

A team member who wishes to change the project approach can submit a change request form through the company's portal or email. The request form will include detailed descriptions such as project name, date, requester, priority, change impact, deadline, and comments. The Project Manager is responsible for managing the change log.

3.4.4 Change Request Assessment

The change request will be reviewed by a project manager or technical lead to determine the magnitude of the request. The information of the request be assessed carefully and be determined if it's appropriate to be passed on to the higher management level. If not, the request's owner will be asked to include further information on the request.

3.4.5 Change Request Analysis

This phase is where a final decision on whether the request will be approved or denied by the Change Control Board (CCB). The board will consist of project leaders and technical leaders. Approval from the Change Control Board required an official signed-off from the leader and announced to stakeholders at their meetings. Any changes will be documented on the company's database or any platform the project stakeholders communicate.

3.4.6 Change Request Implementation

After a change request is approved by the Change Control Board, the project will move the request to the implementation phase. At this phase, the stakeholder will work with each other to determine the appropriate timeline and components required for implementation. The project leader will maintain active communication while the project is implementing the change. Changes should be announced throughout the team and recorded on the change log.

3.4.7 Change Request Closure

After the change has been implemented. The project manager is responsible for keeping documentation of the changes. The document should be easy to access and investigated for future work.

4 SCHEDULE/TIME MANAGEMENT

4.1 SCHEDULING METHODOLOGY

This project will employ agile scheduling methodology across several related teams. The teams will pull user stories (elements of the network infrastructure or supply chain) from the customer (the contracted manufacturer) and progressively deliver plans, tools, and systems to support each business segment. Product owners will collaborate with the customer to gather detailed requirements, prioritize the sprint backlog, and coordinate sprints to support scheduling interdependencies. Sprints are defined at one or two-week

periods (depending on scope) and are measured by days.

4.2 SCHEDULE REPORTING

Product owners will report a weekly estimate of sprint progress to the project manager in accordance with the communications plan. The estimate will detail, per task, man-hours scheduled / applied / remaining / variance.

4.3 SCHEDULE CONTROL

The approval authority for schedule changes within the float is the project manager. The approval authority for changes requiring an adjustment to time/cost/quality is the Change Management Board. A variance that consumes more than 25% of float on the critical path requires the Change Management Board to meet and reassess the schedule baseline.

4.4 MILESTONES

4.4.1 - 7JAN - All teams complete onboarding for access to the manufacturer's systems

4.4.2 - 21JAN - Networking team completes physical inventory of manufacturer on-premises network.

4.4.3 - 28JAN - Contracting team procures manufacturer approval for the scope of changes to the manufacturer's network.

4.4.4 - 11FEB - The Device Monitoring team completes installation of network hardware devices and tests supporting software providing automated accountability of manufacturer's devices. The Supplier Engagement team produces a preliminary HBOM/SBOM for the manufacturer's supply chain.

4.4.5 - 25FEB - The teams publish finalized procedures and guidance (network, onboarding, patching, BOM, threat response)

4.4.6 - 4MAR - Patching team completes installation for automation to segregate non-onboarded systems to a quarantine network.

4.4.7 - 11MAR - The manufacturer successfully tested threat/vulnerability updates and notifications.

4.4.8 18MAR - The Training team verifies that the manufacturer's IT retraining is complete and Cisco staff handoff systems for operation by the manufacturer.

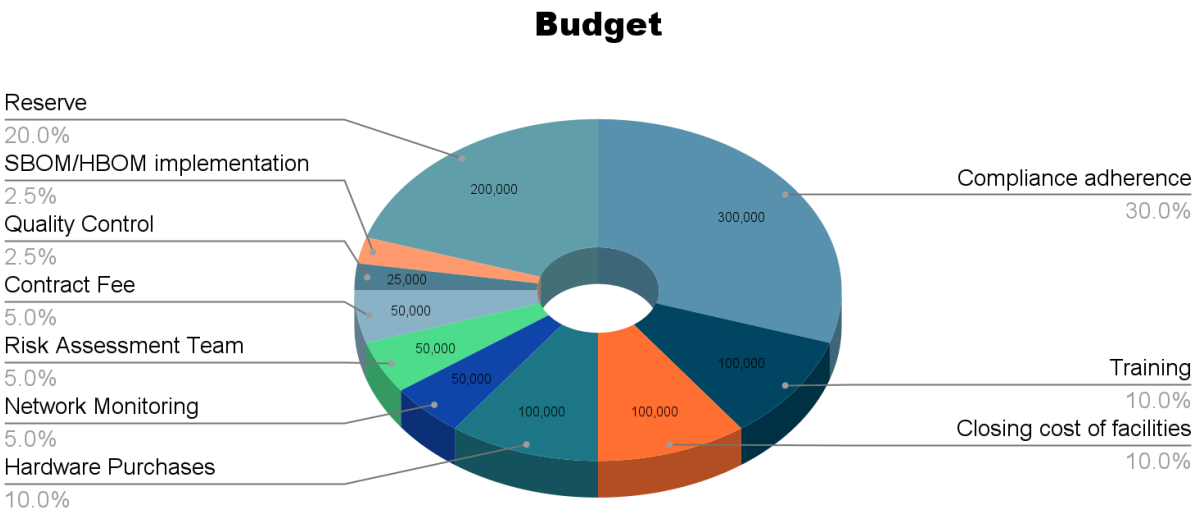
4.5 SCHEDULE BASELINE

See Annex B for the Schedule Baseline.

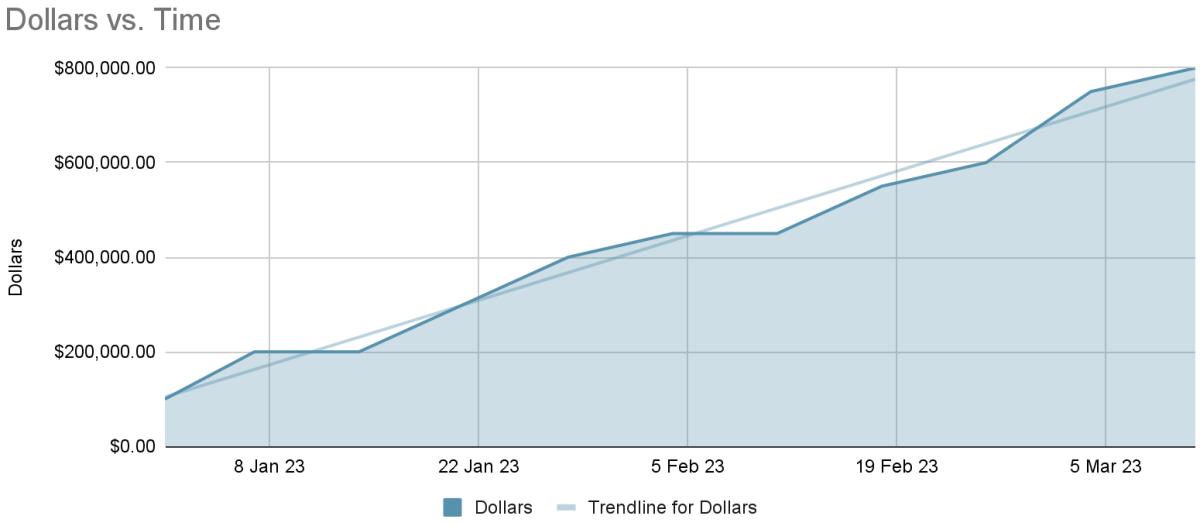
5 COST/BUDGET MANAGEMENT

5.1 Budget

The budget was derived using a Rolling Budget approach. The $1,000,000 budget has been allocated for the training of personnel, compliance adherence, hardware acquisition, research and consultation, and emergency reserve. Cisco leadership has requested tight control over the budget, with remaining funds to be recovered after the 90-day period. Additionally, they have placed a large emphasis on contingency, so we have allocated $200,000 in reserve. The Rolling Budget approach will benefit our project by increasing our month-to-month flexibility and will allow us to revisit the budget as needed. The agility will be critical as production is expected to expand rapidly as we reach project completion. After the 90-day period, we plan to move to a more structured budgeting methodology.



- Compliance adherence 300,000
- Training 100,000
- Closing cost of facilities/contracts: 100,000
- Hardware Purchases 100,000
- Network Monitoring 50,000
- Risk Assessment Team 50,000
- Contract Fee 50,000
- Quality Control 25,000
- SBOM/HBOM implementation 25,000
- Reserve 200,000



*Dollars vs. Time Chart does not include the $200,000 in reserve

6 QUALITY MANAGEMENT

The Cisco Networking Critical Infrastructure Supply Chain Risk Management project team will incorporate an efficient framework that adheres to the guidelines and protects the integrity of Cisco's products and systems. Quality management will help Cisco meet domestic production standards, also those set by Cisco as one of the top corporations within the digital communication technology industry.

As challenges arise, the Quality Management team will adjust controls to overcome these obstacles. Efficient, rapid evaluation and adjustment of quality management will be needed to help for a swift transition to domestic production without affecting Cisco's production and economic profits.

6.1 Quality Objectives, Standards, and Approaches

Cisco will follow ISO 9001:2015 as our Quality Management System. This standard covers all the main components to ensure the success of our project. We will use this system to fulfill our needs and focus on the following.

- Improvement
- Evidence-based Decision Making
- Relationship Management
- Process Approach

Using ISO 9001 will engrain a constant quality loop with the new producer, reducing the number of production errors and raising overall customer satisfaction. Additionally, it should help us reduce excess budget expenditures on underperforming staff or products.

We are not seeking ISO 9001:2015 certification at this point in the project.

6.2 Cost of Quality

- Following this standard will help implement a practical budget and also an efficient team to continue the top quality of products produced by Cisco.

6.3 Total Quality Management

- ISO 9001:2015 focuses on creating satisfied customers, management, and employees, continuously improving their processes, and overall saving cost.

6.4 Continuous Quality Monitoring

- As stated in ISO 9001: 2015, this standard applies to any organization to create a standard for quality management organizations and systems. This will allow for efficient productivity and promote accountability within the organization.

7 COMMUNICATIONS MANAGEMENT

7.1.1 Stakeholder communications requirements:

- **Closely manage (CM)** individuals who have high power and are highly interested in the project, such as your boss.
- **Keep satisfied (KS)** the individuals with high power and less interest in the project, but don't overwhelm them with information.
- **Keep informed (KI)** individuals with low power but who are highly interested in the project's details.
- **Monitor (MR)** individuals with low power and who are less interested and don't provide excessive communications.

7.2.1 Communications summary:

Stakeholders	Communications Type	Delivery Method/Format	Producer	Due/Frequency
Sundar Agrawal (*CM*)	Monthly-status/forecast/earned value report	Hard copy Short meeting	Ethan Nesel	1ST Thursday of month at 10 AM
Jon Davidson (*KS*)	Monthly- Updates	E-mail intranet site	Ethan Nesel	1ST Thursday of month at 10 AM
Elon Sumk (*KS*)	Monthly- Updates	E-mail intranet site	Ethan Nesel	1ST Thursday of month at 10 AM
Jon Boyens (*KS*)	Monthly- Updates	E-mail intranet site	Ethan Nesel	1ST Thursday of month at 10 AM
Angela Smith (*KI*)	Weekly- status report	Hard copy Short meeting	Team Lead	Wed. mornings 9 AM
Huong Trinh (*KI*)	Weekly- status report	Hard copy Short meeting	Team Lead	Wed. mornings 9 AM
Dr. Ron Ross (*KI*)	Weekly- progress report	Hard copy Short meeting	Team Lead	Wed. mornings 9 AM
John Roberts Jr. (*KI*)	Weekly- progress report	Hard copy Short meeting	Team Lead	Wed. mornings 9 AM
Scott Liang (MR)	Project announcement	Memo, e-mail, intranet site, and announcement at department meetings	Ethan Nesel	Kick Off Meeting
Project team (MR)	Weekly-status/progress report	Short meeting	All team members	Tues. afternoons at 2:00 (Scrum Stand-up)

7.3.1 Comments/Guidelines:

- **Status:** reports the current process performance against the performance measurement baseline
- **Progress:** outlines total work accomplished
- **Forecasting:** future project status and performance based on current or historical data
- **Earned Value:** reviews scope, cost, and schedule measures to assess project performance

7.4.1 Escalation procedures for resolving issues:

Priority	Definition	Decision Authority	Timeframe for Resolution
Priority 1	Major impact to project or business operations. If not resolved quickly, there will be a significant adverse impact on revenue and/or schedule.	Vice President or higher	Within 4 hours
Priority 2	Medium impact to project or business operations which may result in some adverse impact to revenue and/or schedule.	Project Sponsor	Within one business day

Priority 3	Slight impact which may cause some minor scheduling difficulties with the project but no impact on business operations or revenue.	Project Manager	Within two business days
Priority 4	Insignificant impact on to project, but there may be a better solution.	Project Manager	Work continues, and any recommendations are submitted via the project change control process

8 RISK MANAGEMENT

In order to minimize the risk of supply chain threats pertaining to overseas production of critical infrastructure hardware, this project will assess the feasibility of producing Cisco hardware in the US. In an effort to minimize the risk associated with moving all production to the US, this project is a smaller-scale proof of concept. In case of project failure, Cisco can fall back onto its current method of developing hardware overseas.

For the scope of this project, Cisco will focus on selecting and supporting an external vendor in ensuring that their SBOM and HBOMs meet the criteria set forth by government regulations and Cisco. Despite the small scope of this project, there are risks that should be kept in mind.

8.1 VENDOR COMPLIANCE

The 3rd party vendor that Cisco will be supporting to produce Cisco hardware must successfully meet the compliance requirements set forth by the US government regulations and Cisco. The vendor must meet E.O. 14017 and E.O. 14088 requirements and be able to remediate or mitigate critical known vulnerabilities.

In order to protect Cisco's intellectual property regarding the designs of its products, the vendor must also sign all required legal documents and contracts, including a non-disclosure agreement (NDA).

8.2 DEFENSE IN-DEPTH

Cisco must be able to safeguard its intellectual property. As such, the vendor must only be able to access the documents necessary to create the approved router and/or switch. Access will be provided and managed by Cisco to the vendor and its employees. Cisco will use the Principle of Least Privilege to ensure the confidentiality of its product designs.

Any access to Cisco documentation, systems, and design must be controlled using Multifactor Authentication (MFA). The vendor must also use MFA and secure authentication whenever dealing with Cisco's Intellectual property.

As part of the defense-in-depth initiative, regular audits of all security processes must be conducted internally. Any sensitive data stored outside of Capital One systems must be encrypted at rest and in transit.

8.3 REGULATORY NOTIFICATION

In case of breach or loss of data that may affect Cisco's intellectual property, reputation, and financial well-being, Cisco must be notified within 4 hours of discovery. An incident response plan approved by Cisco must be executed to mitigate the impact of the breach. The Vendor must work with Cisco to implement safeguards to prevent future breaches.

The Vendor should also report any breaches to the government within 1 month. Reporting rules may be updated in the future based on changes to internal policy, or local, state, or federal law.

8.4 BUSINESS CONTINUITY PLAN-KEEPING OPERATIONS ONLINE

It is essential business operations continue as normal in the event of a disaster, attack, or failure of systems or processes. In combination with the project team, IT staff, and other related company professionals, the project stakeholders will ensure operations will continue during such events by developing a business continuity plan (BCP). The stakeholders will approve such a plan and be readily available for a business interruption. The BCP, at a minimum, will keep the production of critical infrastructure on track while prioritizing the security of devices and products. The BCP should function to keep critical infrastructure production going until normal operations can continue. It must also be tested using tabletop exercises and unannounced drills twice a year.

8.5 RISK LOG

Risk #	Risk	Risk Type	Risk Description
1	Shortage/Lack of materials	Financial, Resource	The new vendor will have to responsibly source materials that may not be easily available in the US.
2	Lack of US-based vendors	Resource	US-based vendors capable of developing the hardware for Cisco may not be a good fit for the project or not be approved to work with Cisco due to relations with competitors and other factors.
3	Delay in legal contracts between Vendor and Cisco	Scheduling	A delay in establishing the legal contracts between Cisco and the new vendor may cause delays to the project plan. Conflicts resulting in a contract not being established between the two parties will also result in a delay as Cisco will have to find a new vendor.
4	Development of New US regulations	Compliance	US regulations may change or grow during the course of the project. In this case, the requirements set forth by Cisco may also need to be updated.
5	Lack of Cisco personnel to support and audit vendors respectively.	Resource	Cisco will need to ensure that they have sufficient personnel to conduct audits on the external vendor as well as personnel to support the vendor in creating their HBOM and SBOMs

Risk #	Risk	Risk Type	Risk Description
6	Lack of knowledge/experience to build Cisco hardware	Scheduling	Lack of knowledge in building Cisco Hardware will require additional training for the workers as well as a decline in the number of units that are produced.
7	Safety control implementation and verification	Scheduling, Financial	US safety regulations must be understood, implemented, and have their implementation verified. Unsafe practices and equipment must be replaced, which can lead to delays in production and additional cost
8	Higher costs in sourcing materials locally	Financial	Higher costs in sourcing materials locally will result in Cisco paying more to produce the routers and switches.
9	SBOM/HBOM Management Tooling	Financial, Scheduling	The external vendor may not have approved tooling to manage their SBOM and HBOMs. Cisco may need to support the vendor in selecting the proper tooling

Appendix A: Project Management Plan Approval

The undersigned acknowledge they have reviewed this Project Management Plan and agree with the approach it presents. Changes to this Project Management Plan will be coordinated with and approved by the undersigned or their designated representatives.

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____