The Digital Manufacturing Institute

MxD Final Report Project 20-01-A

CIRI SUPPLY CHAIN ENHANCEMENTS	
Principle Investigator / Email Address	N/A
Project Team Lead	HEARTLAND SCIENCE & TECHNOLOGY GROUP
Project Designation	20-01-A
UI LABS Contract Number	2020-05
Project Participants	HEARTLAND SCIENCE & TECHNOLOGY GROUP
MxD Funding Value	N/A
Project Team Cost Share	N/A
Award Date	07/13/2020
Completion Date	04/30/2022

This project was completed under the Technology Investment Agreement No. W15QKN-19-3-0003, between Army Contracting Command – New Jersey MxD. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of the Army.

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED

mxdusa.org
@mxdinnovates
info@uilabs.org

1415 N. Cherry Avenue
Chicago, IL 60642
(312) 281-6900

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2
Dashboard Background 3
II. Project Deliverables 3
III. PROJECT REVIEW 4
Use Cases & Problem Statement 4
Scope & Objectives 4
Technical Approach 4
Planned Benefits 20
IV. KPI'S & METRICS 21
V. TECHNOLOGY OUTCOMES 22
Technology Deliverables 22
System Overview 22
System Requirements 22
System Architecture 22
Features & Attributes 22
Target Users & Modes of Operation 22
Software Development/Design Documentation 22
VI. INDUSTRY IMPACT 22
VII. TRANSITION PLAN 23
Transition Chart 23
Transition Summary 23
Recommended Sequence of Use 23
Next Steps & Challenges 23
VIII. WORKFORCE DEVELOPMENT 23
IX. CONCLUSIONS & RECOMMENDATIONS 23
X. LESSONS LEARNED 24
XI. ACCESSING THE TECHNOLOGY 24
XII. DEFINITIONS 24

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED

mxdusa.org
@mxdinnovates
info@uilabs.org

1415 N. Cherry Avenue
Chicago, IL 60642
(312) 281-6900

I. EXECUTIVE SUMMARY

The Cyber Secure Dashboard (Dashboard) is a cloud-based application that operationalizes a sound, standardized cyber risk management process. It provides enterprises with detailed documentation, guidance, policies, reports, standards, assessment methodologies, and tracking mechanisms to comply with government mandated cybersecurity requirements for information systems that store and process controlled unclassified information (CUI) or other sensitive data. The Dashboard is designed to facilitate long-term compliance, cybersecurity awareness throughout the organization, and the sharing and vetting of an organization's cybersecurity posture with all stakeholders, including government contracting officers, prime contractors, and insurance providers. It also provides policy templates, best practices tailored to the specific controls required (and recommended) by the government, an integrated task management system, and other features to facilitate the assessment, monitoring, and management of an organization's cybersecurity policies and procedures.

At its most basic level, the Dashboard provides organizations with the ability to continually assess their cybersecurity status according to nationally established standards and to develop a plan of action to maintain and improve their cybersecurity posture. To this end, the Dashboard incorporates the following cybersecurity standards and assessment methodologies that were developed by the Department of Defense (DoD), the National Institute of Standards and Technology (NIST), and the Department of Homeland Security (DHS).

Under contract to MxD, Heartland Science and Technology Group (Heartland) added support for supply chains within the Dashboard. The objective of this functionality is to provide an aggregated view of the cybersecurity posture for a supply chain (or other groupings) of organizations (see Figure 1). This is accomplished by allowing Dashboard account owners to

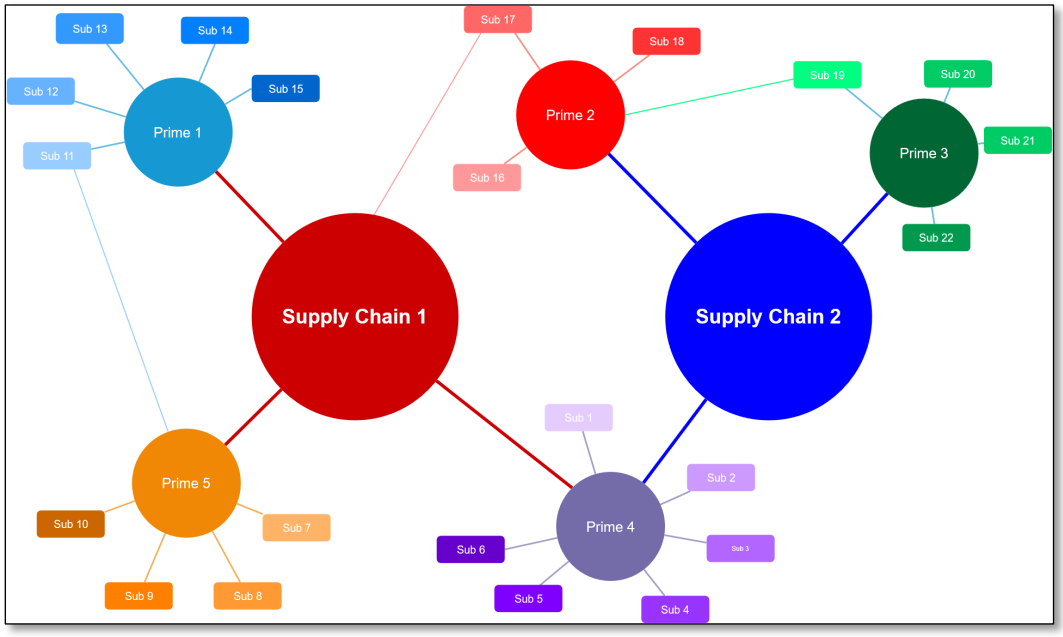

Figure 1. Supply chain aggregation.

selectively share their cybersecurity posture with other Dashboard account owners in a secure manner. As illustrated in Figure 1, a supply chain includes multiple levels of suppliers and prime

contractors that themselves can be suppliers to others within the supply chain. The implementation approach used to create an aggregated supply chain score, and the methodology employed to avoid double counting organizations within a supply chain, are summarized below.

DASHBOARD BACKGROUND

In 2015 the Department of Defense issued a modification of the DFARS (DFARS 252.204-7012) which mandated that all DoD contractors meet heightened cybersecurity requirements, specifically citing the security controls outlined in the NIST Special Publication 800-171 as the criteria for compliance.

The release of the Framework and the DFARS modification created the need to help manufacturers – particularly small and medium enterprise (SME) manufacturers – meet the requirements established by NIST SP 800-171 and to move toward conformance with the NIST CSF. Meeting that need requires a solution based on a solid understanding of the goals and objectives of the processes outlined in the NIST CSF, and the specific security controls identified in the NIST 800-171, balanced against the real-world operational needs and constraints of the manufacturers and the manufacturing supply chains. The solution would need to be developed, tested, and delivered to market in a commercially sustainable manner.

In June 2016, the Information Trust Institute at the University of Illinois at Urbana-Champaign (UIUC) was awarded a research grant by the Digital Manufacturing and Design Innovation Institute (DMDII) to develop a tool that would reduce the burden on SMEs in meeting the new DFARS requirements. This project marks the starting point of the Dashboard. Subsequently, the Dashboard has matured through additional funding, primarily from the Department of Homeland Security (DHS) through it Critical Infrastructure Resilience Institute (CIRI) at the University of Illinois.

II. PROJECT DELIVERABLES

The following list includes all deliverables created through this project. These deliverables will be referenced throughout this final report and can be accessed on the membership portal in accordance with the rights defined in the Membership Agreement.

#	Deliverable Name	Description	Deliverable Type
1	Role Permissions Matrix	User & account permissions definitions	Document
2	Design Documentation	Back-end development documentation (incorporated into the final report)	Document
3	User Guides	How-To documentation (incorporated into the final report)	Document
4	Docker Containers	Software package	N/A
5	Final Architecture Document	Describes the supply chain model (incorporated into the final report)	Document
6	Usability Testing	(MxD did not provide testers)	N/A
7	Final Report	Project summary	Document

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED

III. PROJECT REVIEW

USE CASES & PROBLEM STATEMENT

The objective of this project was to provide an application to continuously assess and quantify the cybersecurity of an entire supply chain for without exposing proprietary and sensitive corporate self-assessment data and supply chain relationships. This objective becomes challenging due to the facts that 1) the organizations within a supply chain may employ different cyber security standards and assessment methodologies, 2) suppliers can provide services to multiple organizations within the supply chain and at different levels within the supply chain, and 3) two organizations can be both a supplier and a prime (or client) to the other.

Additionally, the goal of this project was to aggregate the supply chain cyber security status at a cybersecurity Standard level in order to identify problem areas and develop solutions, which could range from training and assistance to financial and contractual incentives.

This project targeted the following key use cases:

1. As a large aerospace company product manager, I want to assess the cybersecurity risks in my supplier and act, as needed, to correct the weak areas.
2. As a government buyer, I want to monitor the cybersecurity status of the supply chains for the products I purchase.

SCOPE & OBJECTIVES

The objective of this project was to add a supply chain capability to the Cyber Secure Dashboard. The scope of the work included the following:

1. A mechanism to “link” or connect supplier and client supply chain accounts.
2. An automatic aggregation of cybersecurity of linked accounts.
3. A secure method to aggregate and share data.
4. Methods to visualize and analyze the results.

TECHNICAL APPROACH

To aggregate the cybersecurity status of a supply chain, it is necessary for supply chain members to share data. The Dashboard does this in a secure manner using a public-private key pair encryption methodology that requires direct confirmation between the sharing organizations before data can be transmitted. Furthermore, only general status information (e.g., the number of controls that are implemented, partially implemented, or not implemented) is transmitted to prevent exposing potential cybersecurity vulnerabilities, proprietary information, competition sensitive data, or other sensitive data. Specifically, detailed information such as corporate policies, controls, and configurations are not shared. However, if sharing of detailed information is desired, an organization can provide anyone with read-only or read-write access to their account. Such information, however, is not needed for supply chain status aggregation.

Data Aggregation

The primary objective of the supply chain functionality is to obtain a quantifiable score (based on established cybersecurity standards) of the supply chain in its entirety. However, it is also desirable to obtain insight into the cybersecurity status or vulnerability of the supply chain for

individual, standard-specific requirements in order to understand the actual risks, identify common deficiencies, and develop solutions for resolving those deficiencies, whether it be through education, financial incentives, contracting requirements, or some other method. The aggregation process implemented in the Cyber Secure Dashboard does both.

The key item to note in the data aggregation process is that the results are aggregated

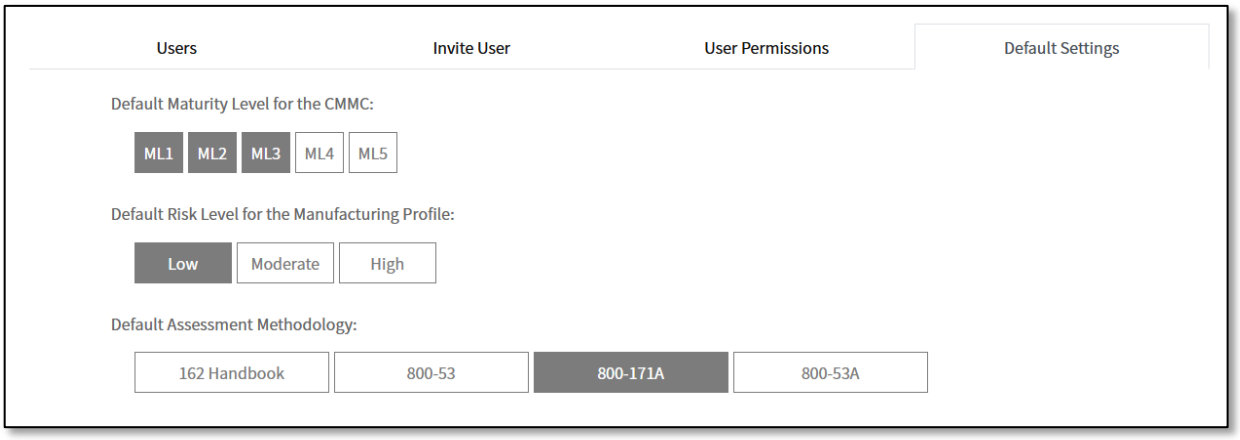

Figure 2. A screenshot of an example account's default settings.

according to the default assessment methodology selected by each organization (see Figure 2). Thus, every supply chain is split into four subgroups – the NIST 800-171A, NIST Handbook 162, NIST 800-53A, and NIST 800-53. Please note that this segregation by assessment methodology is required because it is not possible to force everyone in a supply chain to select a common methodology – a choice that is made individually based on contractual requirements, preferences, or other dictates and incentives.

The aggregated scores are then calculated for each applicable standard as summarized in Table 1. It is important to note that an organization can belong only to one subgroup. This means that the total number of suppliers to any given organization, N_{Total}, is equal to the number of suppliers in each category, or

$$N_{Total} = N_{171A} + N_{HB\ 162} + N_{53A} + N_{53}.$$

For example, the cybersecurity posture for an organization that selected the NIST 800-171A assessment methodology as shown in Figure 2 will be rolled up into DoD CMMC and NIST SP 800-171A standards for each of its' prime contractors (see Table 1). Furthermore, for the DoD CMMC standard, only the scores relevant to CMMC maturity level 3 will be included in this case because of the organization's default setting.

The aggregation process itself is illustrated in Figure 3. In this example, five suppliers form a supply chain in which three of the suppliers employ the NIST SP 800-171A and two employ NIST SP 800-53A assessment methodologies, respectively. Therefore, the compliant, variance, and non-compliant statuses of suppliers 1-3 are applicable only to DoD CMMC standard, whereas the compliant, variance, and non-compliant statuses of suppliers 4 and 5 are applicable for both the DoD CMMC and NIST CSF standards. The result is that the DoD CMMC requirement AC.1.001 has 3 compliant, 2 variance, and 0 non-compliant scores in its supply

chain, whereas the NIST CSF ID.AM-1 requirement has a score of 1 compliant, 1 variance, and 0 non-compliant.

This process is repeated for each of the requirements in each standard throughout the supply chain. However, in situations where suppliers may appear at multiple points within the supply chain (see, for example, supplier T3-1, T3-2, T3-4, T3-5, and T3-6 in Figure 4), care must be taken to avoid counting a supplier's score more than once, which is accomplished by assigning each supplier a unique ID on the backend server that can be used to remove duplicate entries.

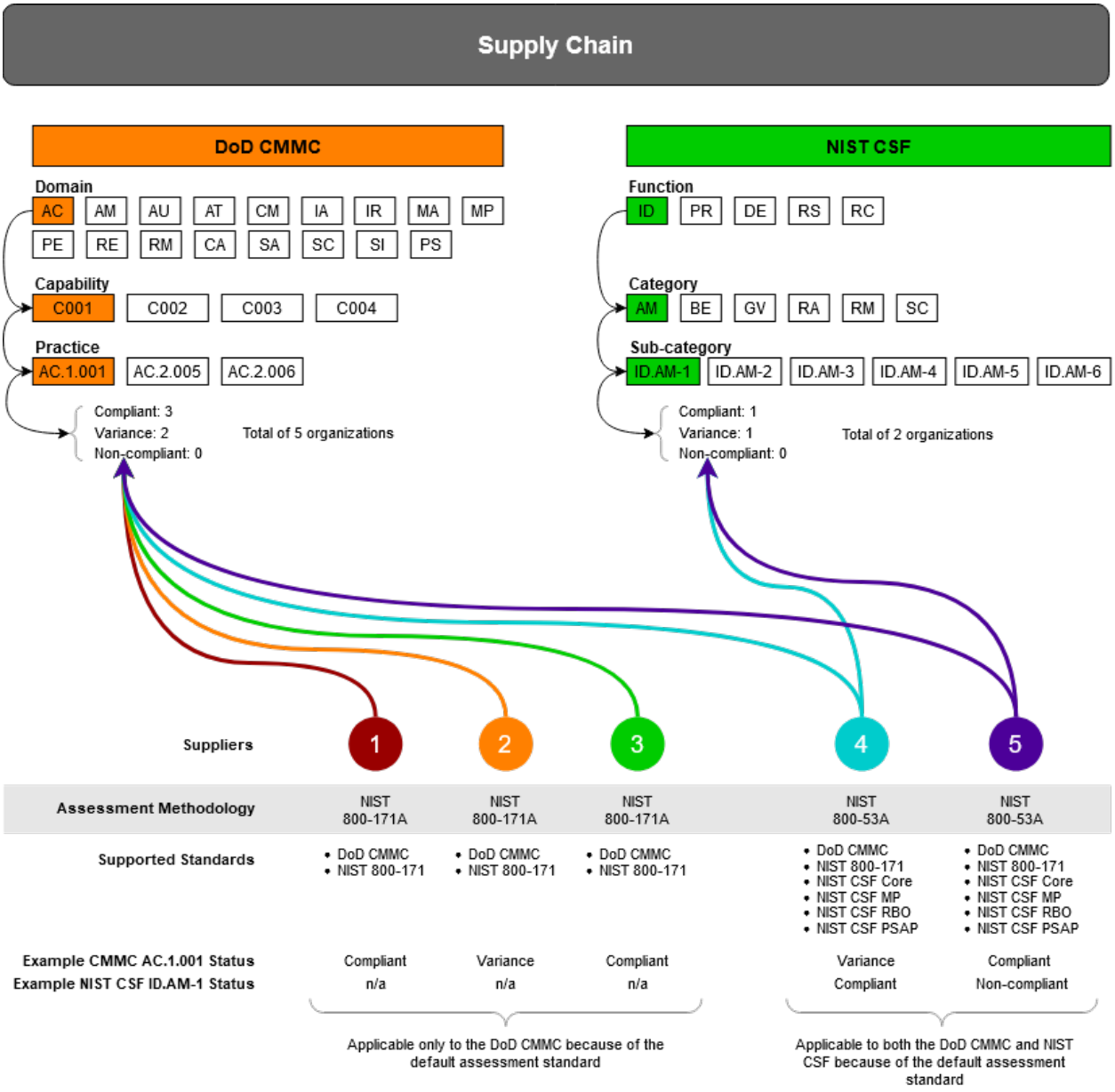

Figure 3. An example of how the cybersecurity status of suppliers is aggregated in the Dashboard.

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED

The last item to note is that the identity of suppliers is known only by those with a direct link. For example, suppliers T2-1 and T1-1 will know the identity of supplier T3-1, but prime contractor P1 will not.

Secure Data Transfer

The Dashboard is a Software as a Service (SaaS) application that is hosted in the Azure Government Cloud to provide the requisite level of security. However, a self-hosted or on-premises solution that is identical to the SaaS solution is also available for organizations wishing to operate their own instance. Therefore, to support supply chains that include both deployment options, the secure data transfer method illustrated in see Figure 5 was implemented. With this approach, a library (also hosted in the Azure Government Cloud) collects the rollup data that has been encrypted prior to transmission from all Dashboard instances. For each Dashboard account, the rollup data is encrypted using the public and private keys that have been added by a Supply Chain administrator. Thus, when the data is archived on the library server, only those members granted explicit permission by the account Supply Chain administration can decrypt the data.

The process by which the rollup data is provided is detailed in Figure 6. The key steps to note in this process are as follows.

1. Rollup data is only sent if two organization elects to share their rollup data with other.
2. Only status information (compliant, variance, or non-compliant) relative to each applicable cybersecurity standard requirement based on an organization's default assessment methodology, CMMC maturity level, Manufacturing Profile risk level, and PSAP category are uploaded.

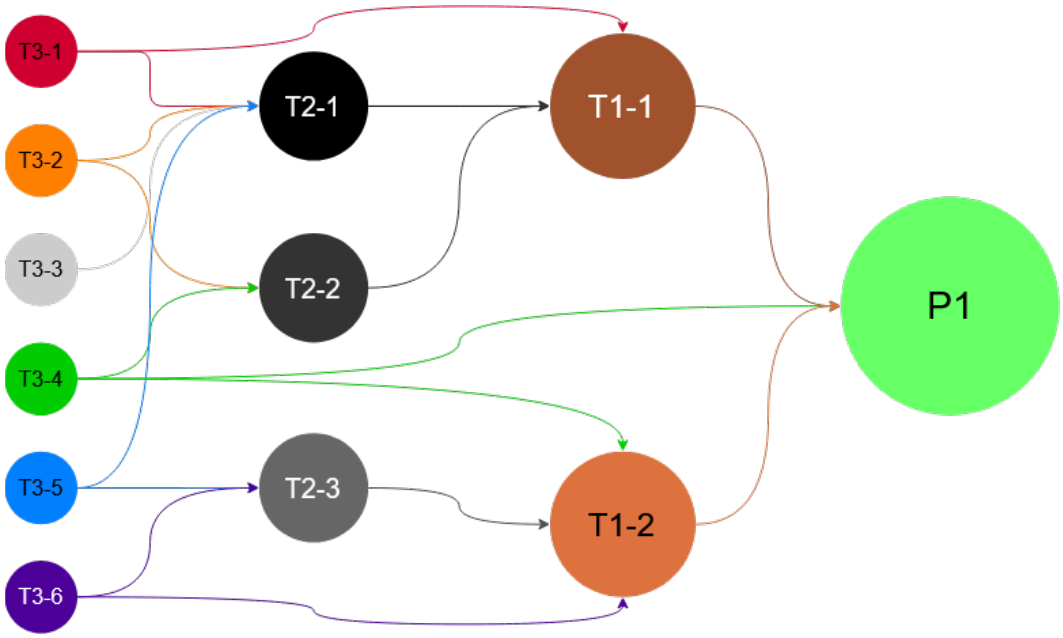

Figure 4. An illustration of a supply chain hierarchy where a supplier may provide goods and services to other suppliers at multiple tiers.

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED

3. All data is encrypted prior to being transmitted using Public Key Encryption. The data will be encrypted using the provider's private key along with all the consumer's public keys. And each time an update is made, the new data will use the latest keys, and exclude any keys removed from the provider's approved list.
4. All data is encrypted such that only the recipients approved by the organization can decrypt it (not even the Cyber Secure Dashboard administrators will be able to decrypt the data).

In addition to the organization's status data, its' supply chain information is also uploaded, which includes the following data.

1. The total number of organizations for each assessment methodology (based on their individual default assessment methodology selection).
2. The resulting total number of compliant, variance, or non-compliant results for each applicable cybersecurity standard requirement (see Figure 3 for an example).

In summary, the rollup data will include the following.

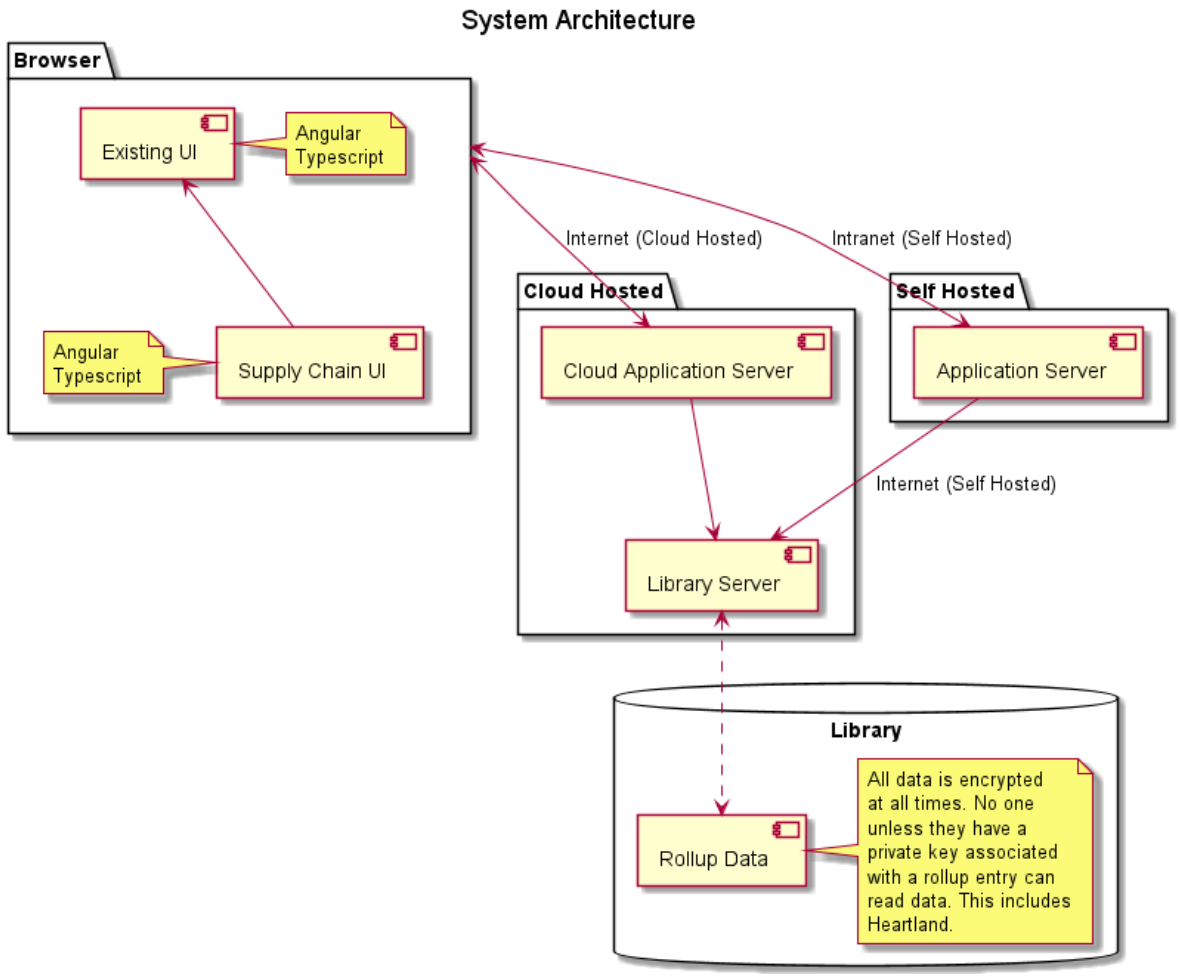

Figure 5. An overview of the supply chain system architecture.

- The total number of accounts (the organization's account and its suppliers).

- For accounts that employ the NIST SP 800-171A assessment methodology, the following data is included.
    - The total number of accounts using the NIST SP 800-171A assessment methodology.
    - The total number of compliant, variance, and non-compliant for each CMMC Practice.
    - The total number of compliant, variance, and non-compliant for each 171 Requirement.
- For accounts that employ the 162 Handbook as their default assessment methodology, the following data is included.
    - The total number of accounts that employ the 162 Handbook methodology.
    - The total number of compliant, variance, and non-compliant for each CMMC Practice.
    - The total number of compliant, variance, and non-compliant for each 171 Requirement.
- For accounts that employ the NIST SP 800-53A assessment methodology, the following data is included.

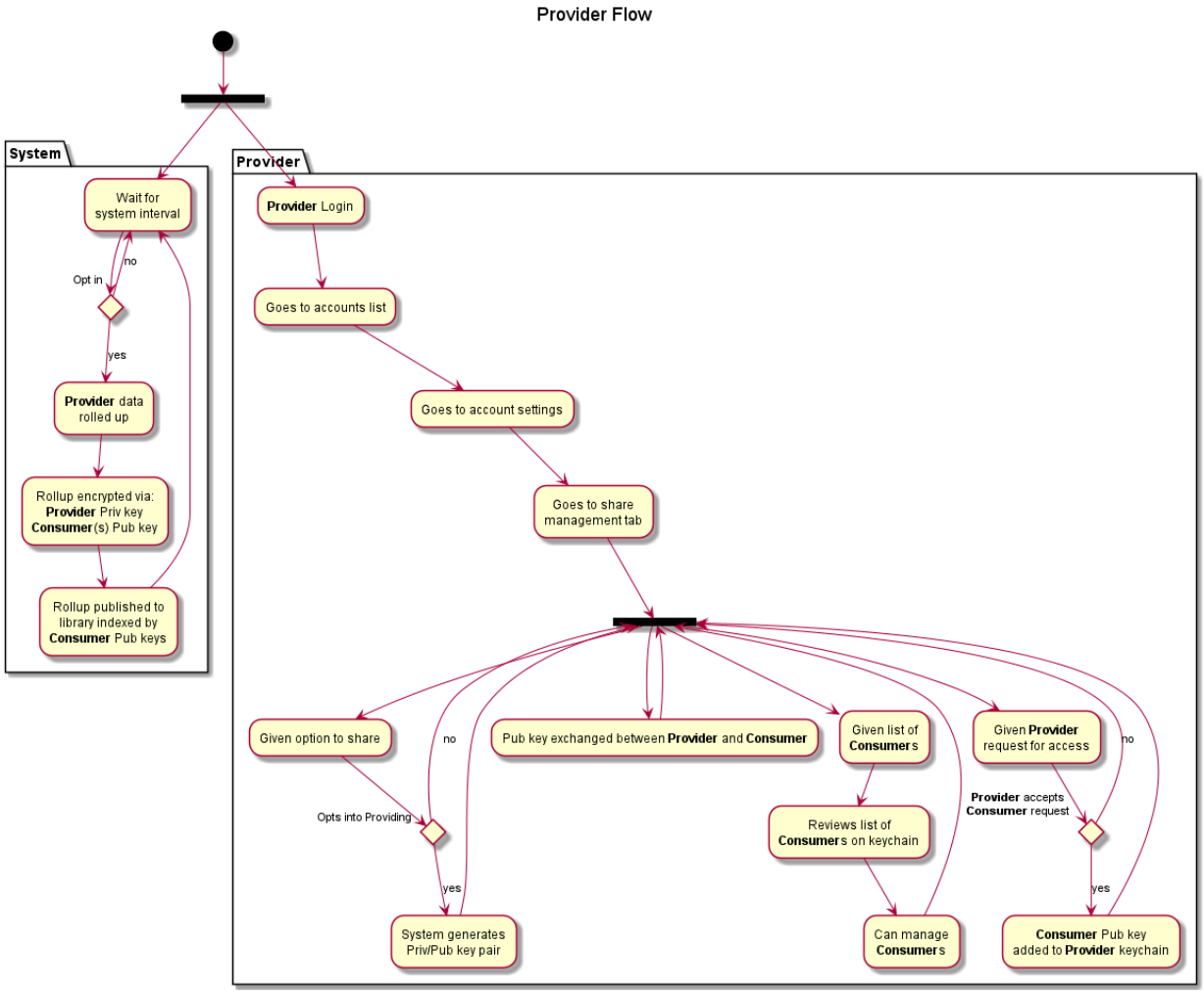

Figure 6. The process by which rollup data is provided.

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED

  - The total number of accounts using the NIST SP 800-53A assessment methodology.
  - The total number of compliant, variance, and non-compliant for each CMMC Practice.
  - The total number of compliant, variance, and non-compliant for each NIST SP 800-171 Requirement.
  - The total number of compliant, variance, and non-compliant for each NIST CSF Core Subcategory.
  - The total number of compliant, variance, and non-compliant for each NIST CSF MP Subcategory.
  - The total number of compliant, variance, and non-compliant for each NIST CSF RBO Subcategory.
  - The total number of compliant, variance, and non-compliant for each NIST CSF PSAP Subcategory.
- For accounts that employ the NIST SP 800-53 as an assessment methodology, the following data is included.
  - The total number of accounts using the NIST SP 800-53 as an assessment methodology.
  - The total number of compliant, variance, and non-compliant for each CMMC Practice.
  - The total number of compliant, variance, and non-compliant for each NIST SP 800-171 Requirement.
  - The total number of compliant, variance, and non-compliant for each NIST CSF Core Subcategory.
  - The total number of compliant, variance, and non-compliant for each NIST CSF MP Subcategory.
  - The total number of compliant, variance, and non-compliant for each NIST CSF RBO Subcategory.
  - The total number of compliant, variance, and non-compliant for each NIST CSF PSAP Subcategory.

With the above information, it is then possible to assess a supply chain's cybersecurity status and to obtain useful metrics at every level within the supply chain. This is performed by each organization at their account level and is achieved by downloading the status information from the library as illustrated in Figure 7. The key points to note are the following.

1. Accounts that have suppliers automatically make a request to the rollup library service (a cloud-based service) to retrieve all rollup packets that they have been granted access to, and their system, whether it is in the cloud or a private instance, will then decrypt the data and make it presentable to the user of the application, based on how they have arranged the accounts in their supply chain.
2. The data provided through the rollup packets provides sufficient information to drill down to the requirements level of each application standard (or dashboard view).

User Interface Enhancement

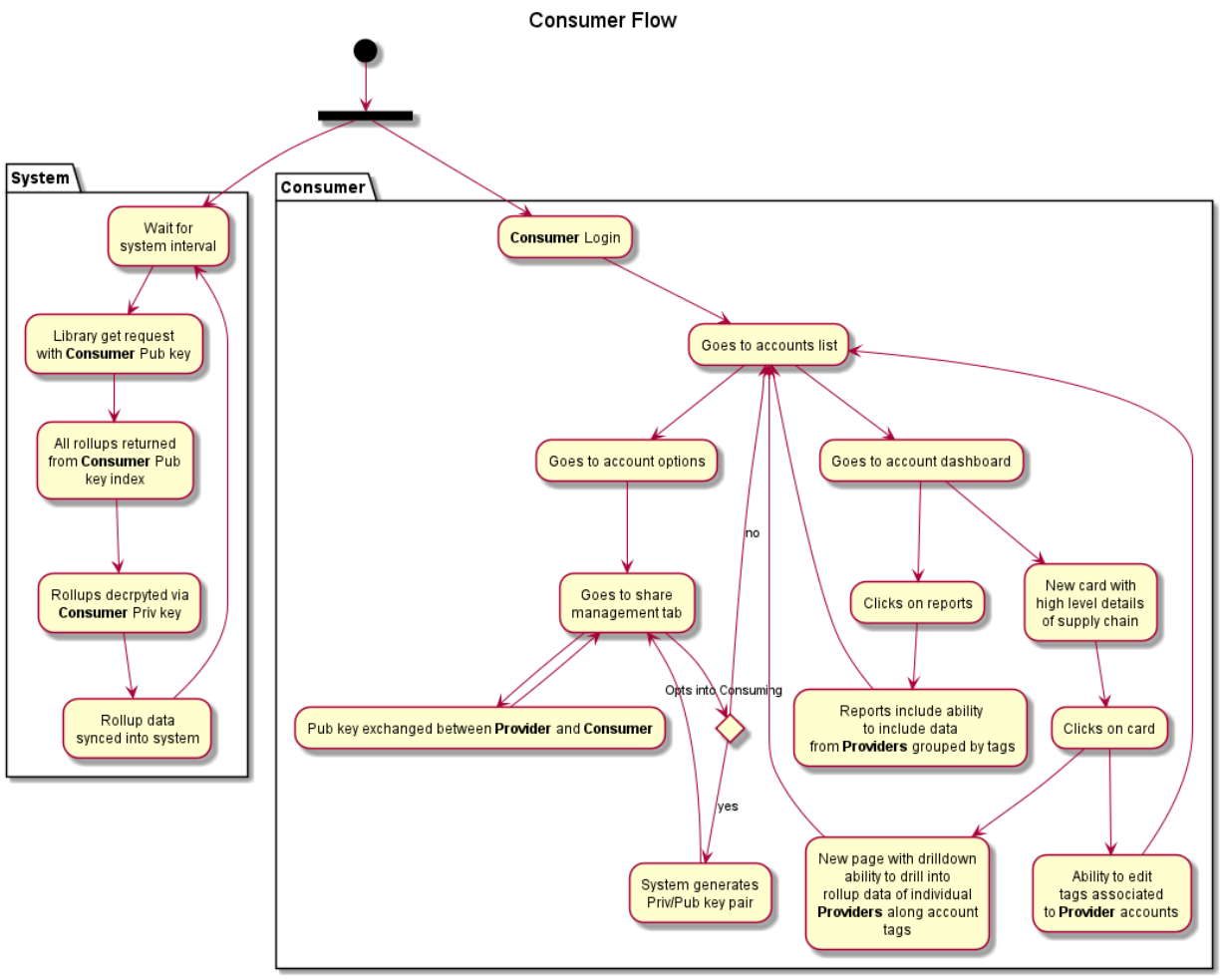

Figure 7. The process by which rollup data is retrieved.

The Cyber Secure Dashboard was modified to provide multiple ways to visualize the data and to download the data in spreadsheet format for detailed analyses. Screenshots of the new user interface are given in Figures 8 – 13. The interface changes begin with the account administration page where a new tab was added to enable/disable account linking (Figure 8). When enabled, a supply chain card is added to the main dashboard page (Figure 9). Clicking on this card or the supply chain link in the left navigation bar will open the main supply chain page (Figure 10). Additional details about the supply chain are available by clicking on one of the graphics (Figure 11). Lastly, the user can view and manage its clients (Figures 12 and 13) and suppliers (Figure 14).

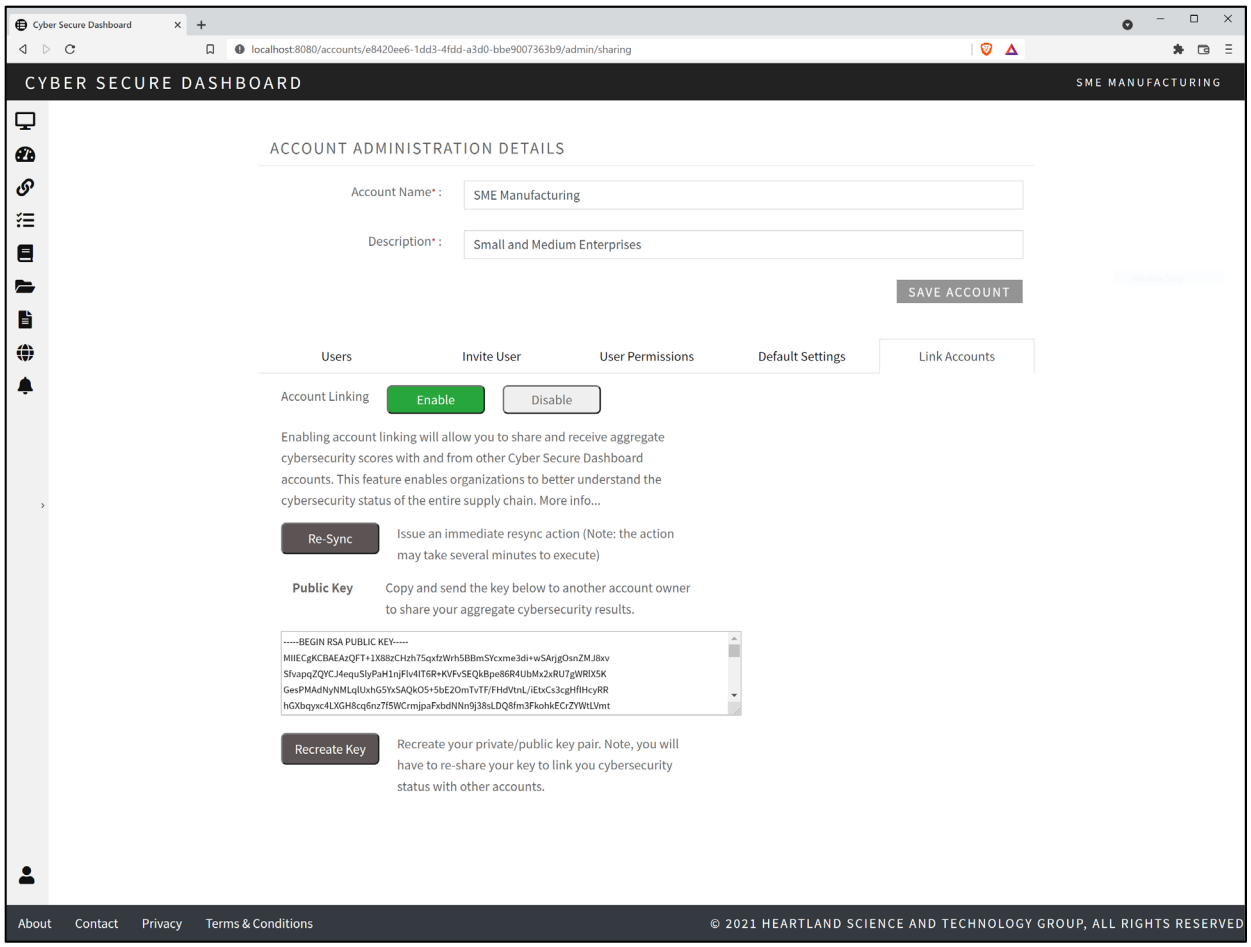

Figure 8. A Link Accounts tab has been added to the accounts screen. Click Enable to turn on the supply chain functionality and share the public key with your direct supply chain members.

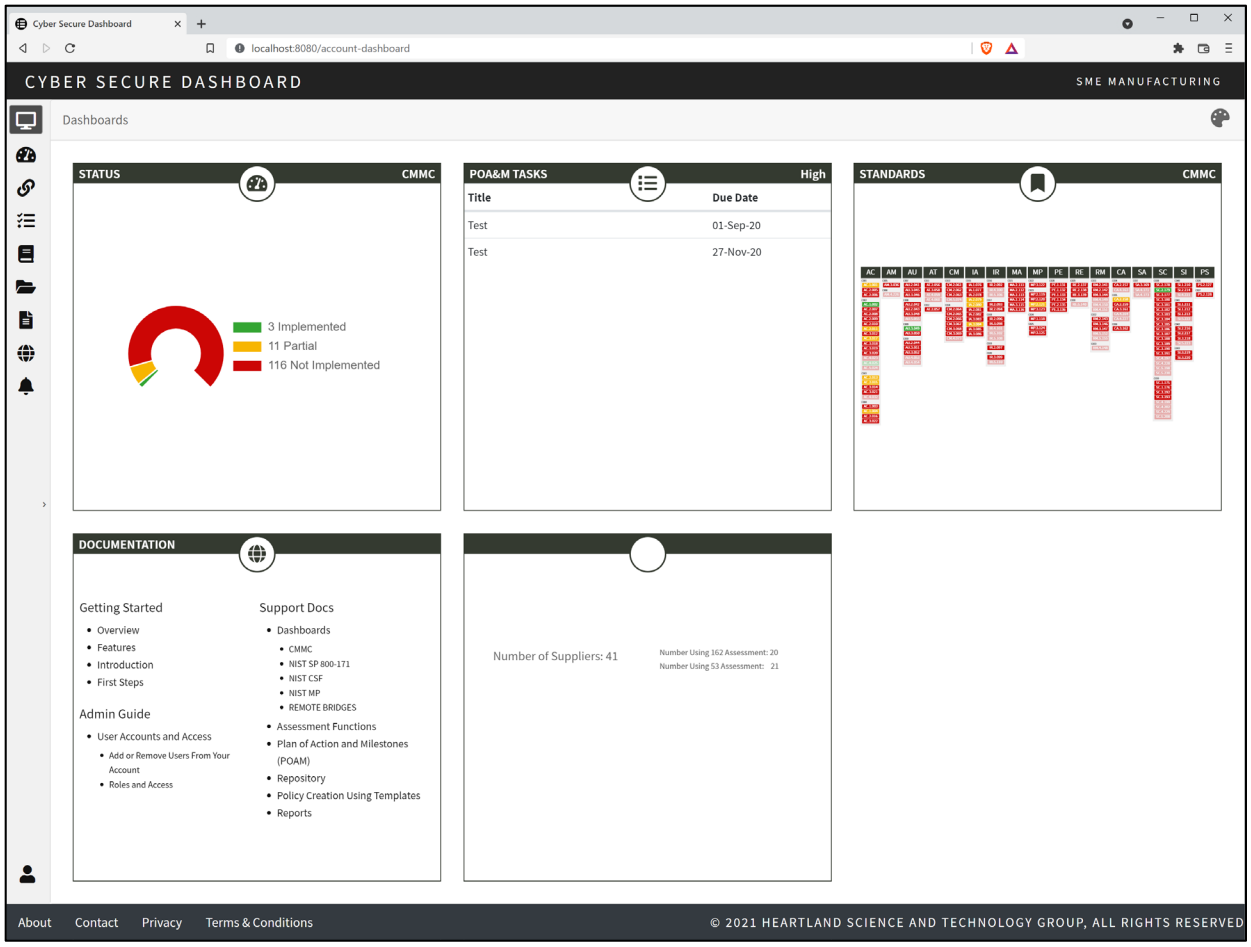

Figure 9. A new Supply Chain card has been added to the landing page along with a new link in the left navigation bar. Click on either one to get more details about your supply chain status.

mxdusa.org
@mxdinnovates
info@uilabs.org

1415 N. Cherry Avenue
Chicago, IL 60642
(312) 281-6900

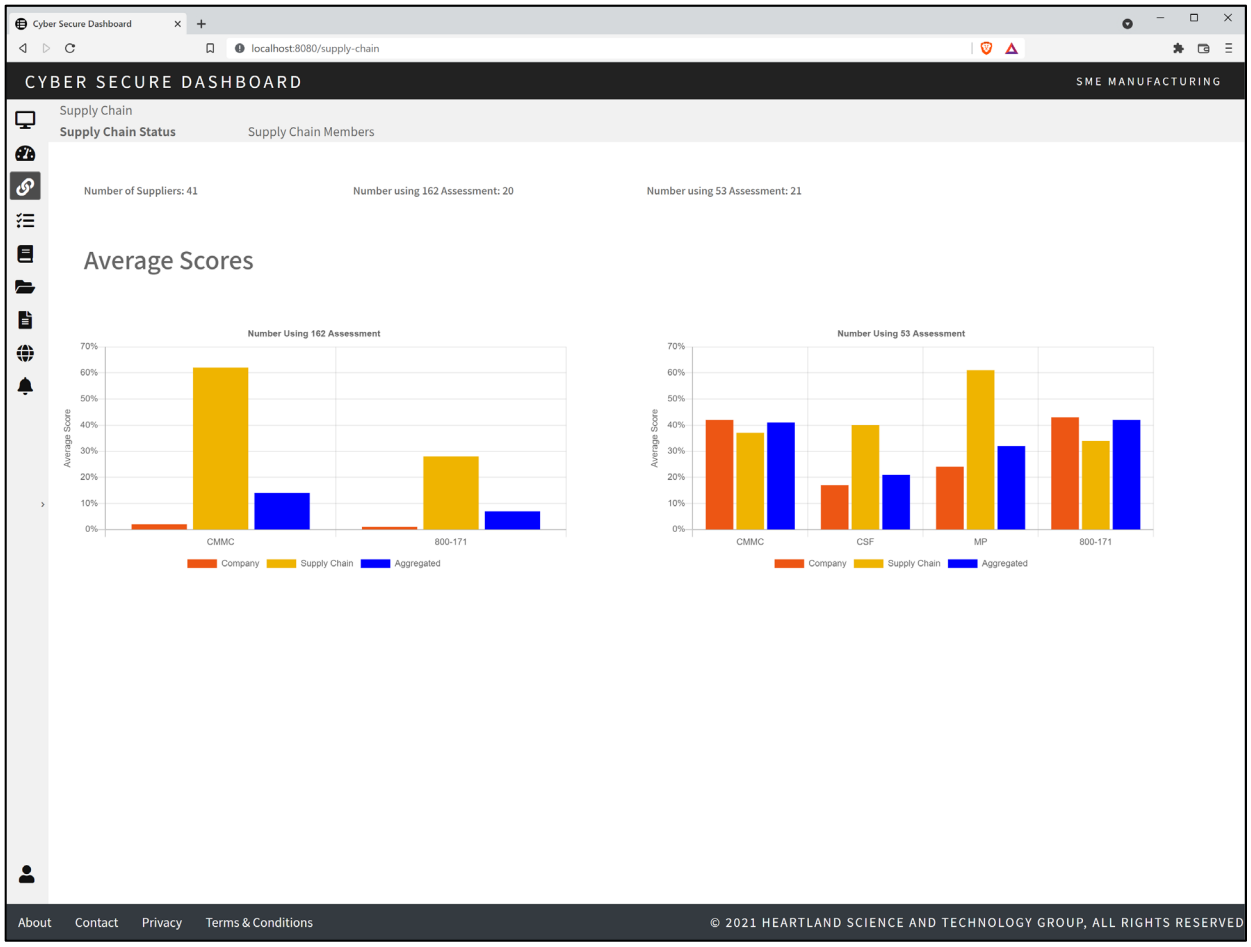

Figure 10. Your supply chain status is grouped by assessment methodology. For each assessment methodology, the supply chain status is shown for all relevant cybersecurity standards. Results are shown for the organization, the supply chain, and the combined aggregated result. Clicking on one of the assessment results will open a new window with more details for that assessment.

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED

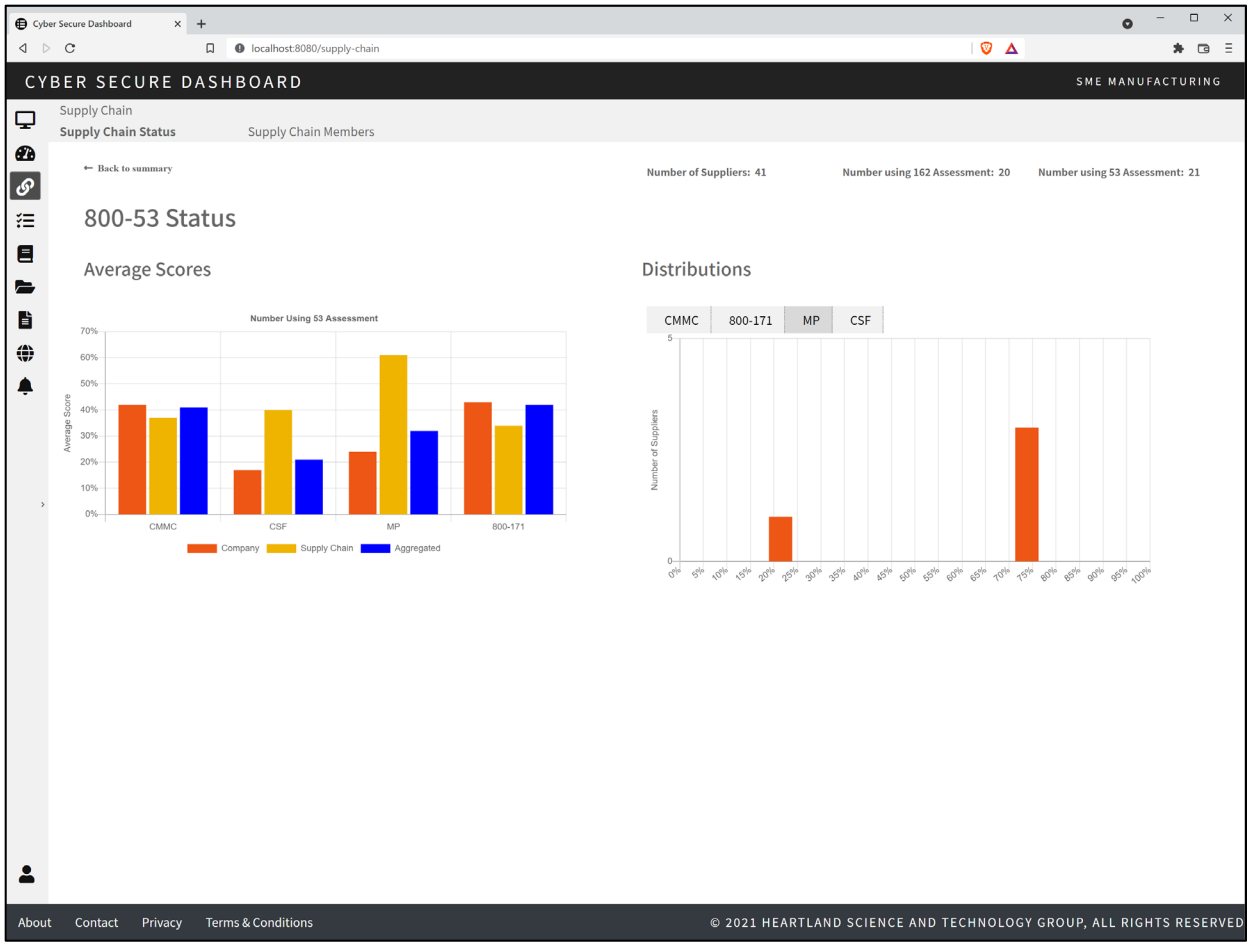

Figure 11. An example assessment view that includes a distribution of the supply chain posture for each of the relevant cybersecurity standards.

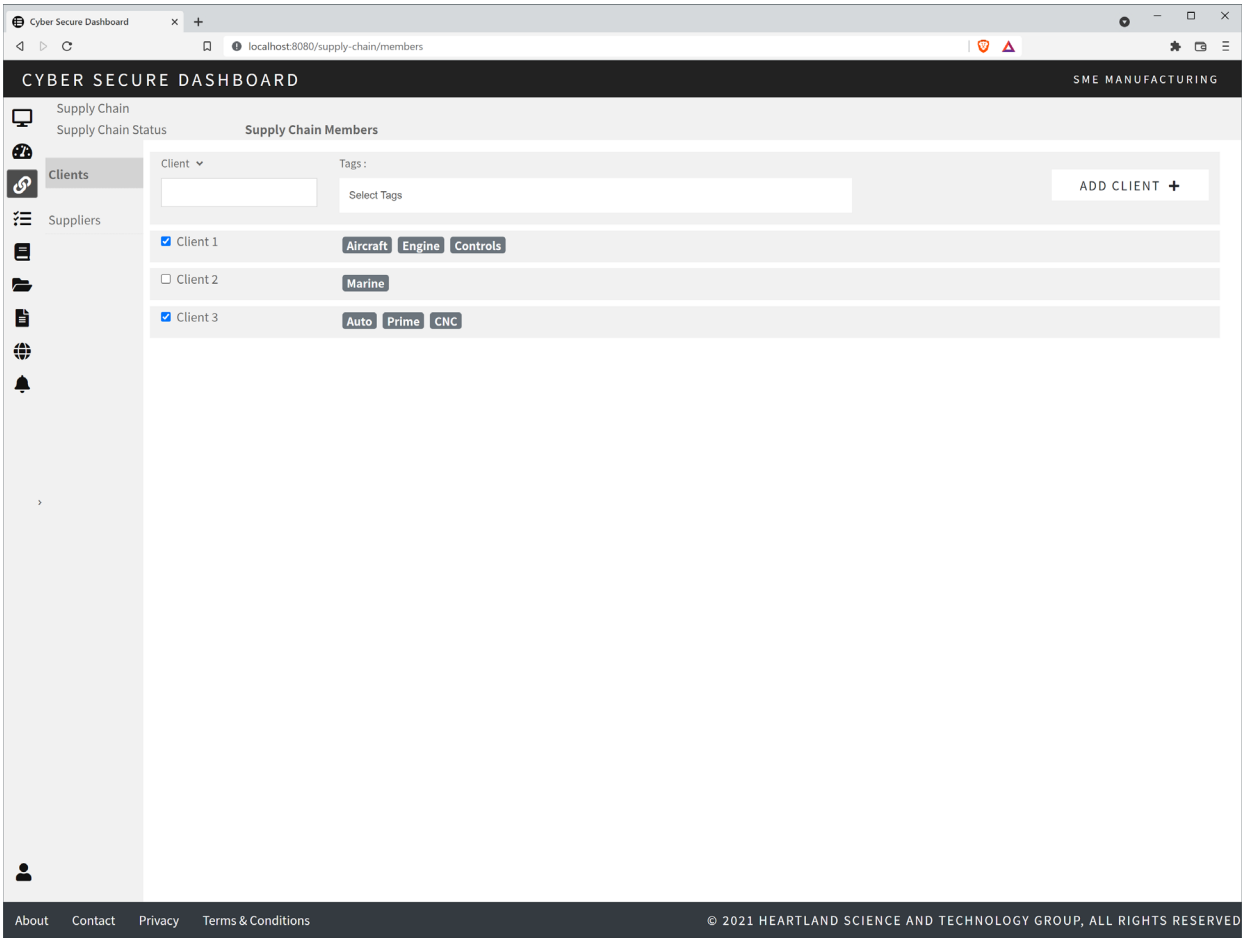

Figure 12. The Clients navigation tab lists the organizations that directly receive your cybersecurity posture. Organizations can be added or remove at will. When adding a new client organization, you will have to supply the organization's public key (see Figure 14).

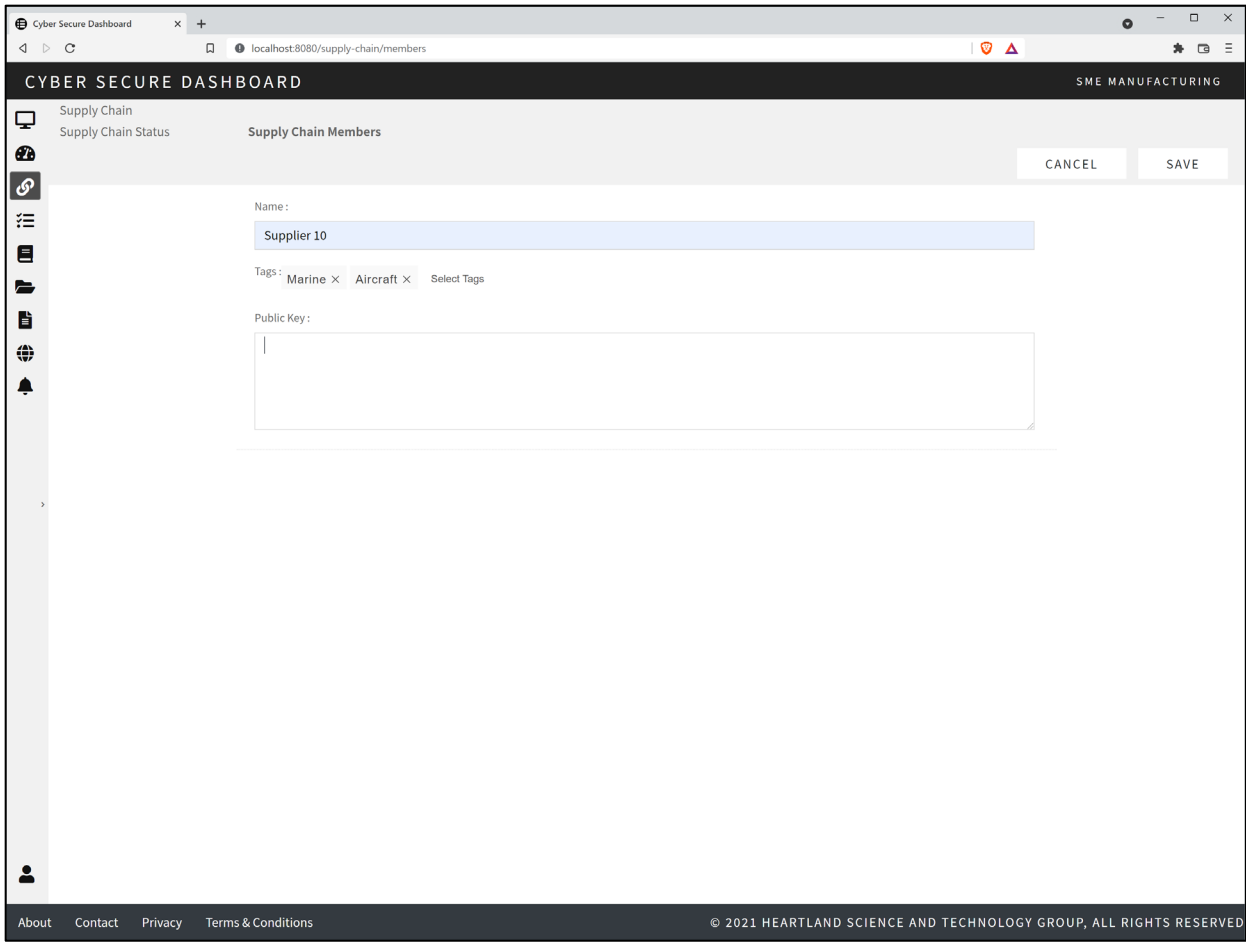

Figure 13. To add a new client organization, the client's public key must be entered. Arbitrary tags can be assigned to filter and categorize your clients.

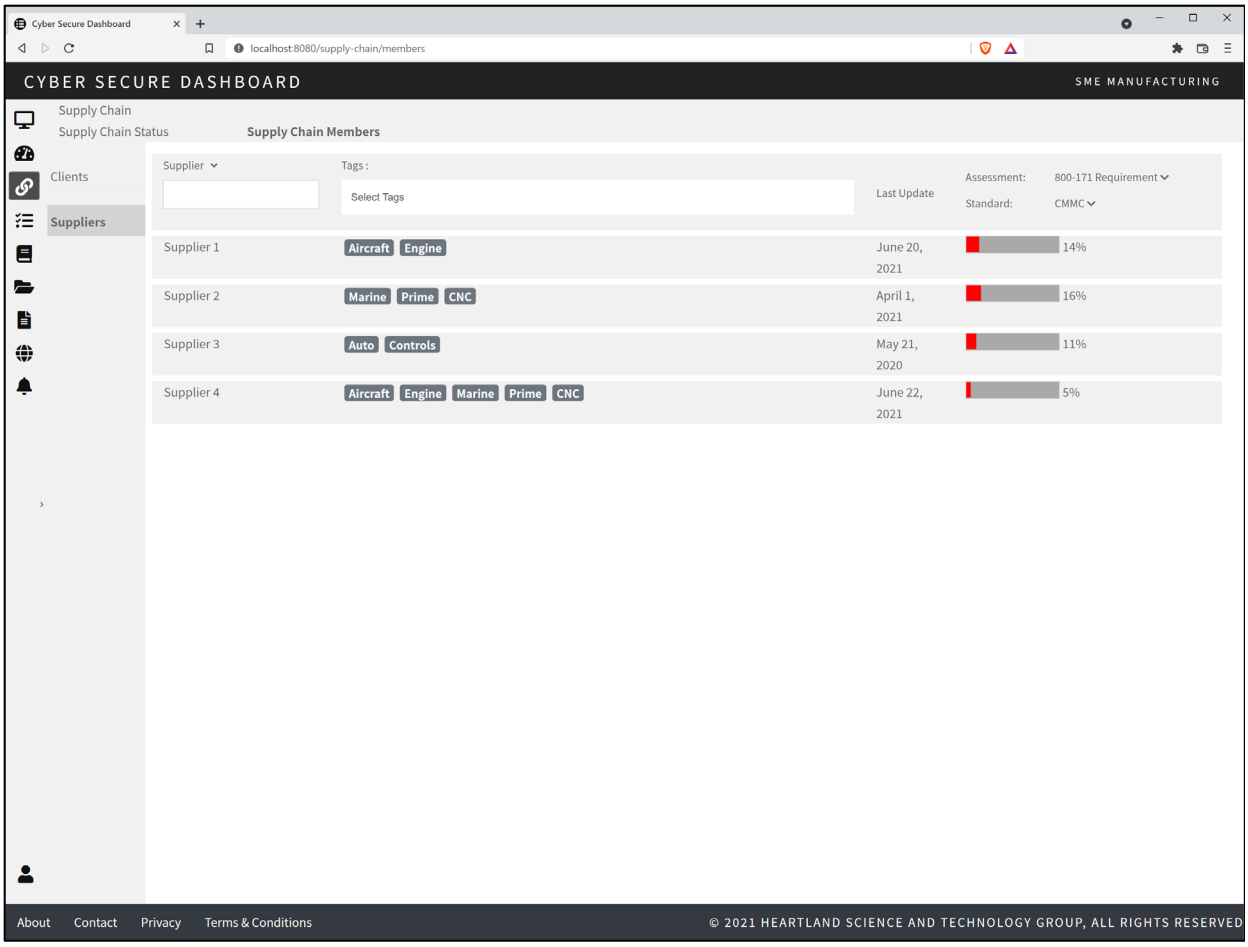

Figure 14. The Suppliers navigation tab lists all your supply chain members and their status. Arbitrary tags can be assigned to filter and categorize your suppliers. Please note that the status of your supplier's suppliers is included in your suppliers' results.

Tasks

Task 1. Implement Linking Functionality

The following tasks were completed:

- A new REST library service to capture and provide encrypted envelopes of supply chain aggregation data was created.
- New user interface functionality as well as backend server functionality to support loading and supplying supply chain data to the library service was implemented.
- A new scheduled task functionality to automatically update supply chain data for accounts was created.

While executing this task, several revisions to the supply chain data structure occurred to support the most effective utilization of the data in the user interface. This effort required refactoring of the codebase to support the changes to the data structure and how results are tallied for an account.

Also, it was decided to transition from RSA encryption to curve25519 encryption for future safety proofing of the encrypted data, which required porting the library service from the .NET Core platform to the Node platform. Likewise, concurrent work on integrating the NIST 800-53A and NIST 800-171A assessment methodologies required enhancing the Supply Chain functionality to support the additional methodologies once the 53A/171A entered our mainline codebase.

Task 2. Roles and Permissions

The dashboard product uses a token to role-based security mechanism, in which different areas of the application have tokens which are then mapped to roles within the system, for a fine-grained control over which roles have access to which parts of the system. We added new tokens, which were applied to existing roles as well as new roles, to manage the security of the Supply Chain feature.

Task 3. Accounts Page Enhancements

A new tab to the account settings which provides access for the user to administrate their supply chain options was added. This page allows the user to enable and disable the Supply Chain functionality, and to also retrieve their public key to share with others for the supply chain linking process.

After starting on this task, changes to the Dashboard to support FedRAMP certification were implemented, which then had to be merged and migrated into the work for the supply chain functionality.

Task 4. Reports Page Enhancements

The ability to export the underlying supply chain data into an Excel formatted document was added, which allows users to perform an in-depth analysis of the supply chain data.

Task 5. Verification and Validation Tests

An extensive, internal verification and validation testing effort was conducted where multiple supply chains were created, and aggregated results were validated. During this process, protection was added to prevent a user duplicating public key entry or using a wrong public key.

Task 6. Post Implementation Support

User support is provided through the normal user support channels of the Cyber Secure Dashboard SaaS application.

PLANNED BENEFITS

The cybersecurity assessment of a supply chain along with a detailed understanding of its weaknesses is required to ensure our products are manufactured correctly and are not subject to cybersecurity attacks. The supply chain functionality provides this capability within a SaaS application that an organization can use to manage all of their cybersecurity policies, procedures, planning, and documentation needs.

IV. KPI'S & METRICS

The table below outlines the key performance indicators and metrics used to evaluate the success of the project outcomes in comparison to the current state and proposed goals.

Metric	Baseline	Goal	Results	Validation Method
Link accounts	Supplier link to a prime or client	Prevent double counting and handle loops	Goal achieved	Generate a supply chain within the Dashboard and tested all of the edge conditions
Aggregate scores	Aggregate scores at the requirement level for all of the standards in the Dashboard	Same	Goal achieved	Validated with the NIST 800-171, NIST CSF, NIST MP, NIST RBO, and DoD CMMC
Securely share data	Encrypt all data	Allow decryption only by parties approved by the account owner	Goal achieved	Backend testing

V. TECHNOLOGY OUTCOMES

TECHNOLOGY DELIVERABLES

#	Deliverable Name	Description	Format of Delivery
1	Dashboard supply chain features	Implementation of a supply chain capability with the Cyber Secure Dashboard	Software as a Service

SYSTEM OVERVIEW

See Technical Approach in Section III Project Review.

SYSTEM REQUIREMENTS

The supply chain capability is provided as a Software-as-a-Service (SaaS) solution. A standard desktop or laptop computer is sufficient.

SYSTEM ARCHITECTURE

See Figure 5, Figure 6, and Figure 7.

FEATURES & ATTRIBUTES

The supply chain functionality has the following features and attributes.

1. The ability for two organizations to share roll-up data, i.e., to “link” their accounts.
2. The ability to link with multiple suppliers and clients.
3. The ability to assess the cybersecurity status of your supply chain categorized by cyber security standard and assessment methodology.

TARGET USERS & MODES OF OPERATION

The supply chain feature is targeted toward product managers, chief technology officers, and others who have the responsibility to ensure that their supply chain is secure and meets specific standards. The Dashboard provides a detailed breakdown of the supply chain results, which can be displayed within the user interface or downloaded for more detailed analysis.

SOFTWARE DEVELOPMENT/DESIGN DOCUMENTATION

The software is web application accessible at https://www.cybersecuredashboard.com. No setup or configuration is required by the end user. Once an account has been created for an organization, an unlimited number of users can be added.

VI. INDUSTRY IMPACT

The supply chain functionality implemented within the Cyber Secure Dashboard provides an easy-to-use mechanism to assess the cybersecurity of a supply chain. Furthermore, since it aggregates the results at a requirement level, it provides the capability to identify specific weaknesses within the supply chain and take corrective action. Furthermore, it does it in a manner where each organization within the supply chain can select one of five different cyber security standards and one of four assessment methodologies.

VII. TRANSITION PLAN

TRANSITION CHART

The transition chart provides a catalog of all of the project deliverables and their respective transition route. Deliverables can transition through deployment at an industry member's site, as an educational reference or through a commercialization effort. Each of these transition routes are detailed in the Transition Summary section below.

#	Deliverable File Name	Technology Integration	Education	Commercialize
1	Role permissions matrix.pdf	X		X
2	Design documentation.pdf	X		X
3	User Guides		X	
4	Final Architecture Document	X		
5	Final Reporting		X	
6				

TRANSITION SUMMARY

The supply chain functionality is available as a commercial product. To use, register for an account at https://www.cybersecuredashboard.com

RECOMMENDED SEQUENCE OF USE

To begin using the supply chain, do the following:

1. Register for an account at https://www.cybersecuredashboard.com
2. Enable the supply chain functionality (see Figure 8).
3. Link accounts (see Figures 12-14).
4. Visualize the results (see Figures 10 and 11).

NEXT STEPS & CHALLENGES

The next proposed step of development is to allow organizations that do not have a Cyber Secure Dashboard account to link their results using a scoring methodology such as the Supplier Performance Risk System (SPRS).

VIII. WORKFORCE DEVELOPMENT

The Cyber Secure Dashboard is being used in community college and other certificate based educational programs, and the supply chain functionality is expected to be incorporated into those programs.

IX. CONCLUSIONS & RECOMMENDATIONS

The Cyber Secure Dashboard operationalizes a sound, standardized cyber risk management process. It provides enterprises with both a process and the details necessary to comply with government mandated cybersecurity requirements for information systems that process and store controlled unclassified information (CUI). In addition, the Dashboard facilitates long-term compliance, cybersecurity awareness throughout the corporation, and the sharing and vetting of an organization's cybersecurity posture with all stakeholders, including government contracting officers, prime contractors, and insurance providers. The Dashboard is based upon the National Institute of Standards (NIST) Cyber Security Framework and includes policy templates and best practices tailored to the specific controls required (and recommended) by the government.

With the addition of the supply chain functionality, the Cyber Secure Dashboard provides the mechanism to aggregate and assess the cybersecurity posture of large, complex supply chains.

It is recommended that MxD establish a beta-test program to test the supply chain functionality as well as the benefits of using the Dashboard to conduct standardized assessments and manage cybersecurity procedures. In addition, it is recommended that the supply chain functionality be extended to import data from organizations that do not subscribe to the Dashboard.

X. LESSONS LEARNED

The two primary lessons learned are the following:

1. The aggregation of the supply chain results proved to be much more difficult than expected because of the complex relationships that are possible within a supply chain and the need to protect proprietary supply chain relationships.
2. The aggregation was further complicated by the need to support multiple assessment methodologies.

XI. ACCESSING THE TECHNOLOGY

The supply chain functionality does not require any specific background intellectual property or capabilities. To get the maximum use out of the supply chain, an organization should conduct their own cybersecurity assessment within the Cyber Secure Dashboard and ask their suppliers to do the same.

XII. DEFINITIONS

What follows are a set of definitions, terms, and acronyms used in this document. These definitions were gathered from various source including the internet, reference papers, standards organizations, and the authors of these documents.

[Term/Acronym] – Definition or description

CMMC stands for the Cybersecurity Maturity Model Certification, a comprehensive framework developed by the Department of Defense to protect the defense industrial base from cyber threats.

CUI stands for Controlled Unclassified Information, which is defined by the National Institute of Standards and Technology (NIST) as “Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.”

REST refers to a RESTful Application Programming Interface (API), which is an API that conforms to the representational state transfer architecture style.