Proof Of Concept
For An ICT SCRM
Enterprise Assessment Package

Supply Chain Management Center
RH Smith School Of Business
University Of Maryland College Park

Final Report
Submitted To: Mr. Jon Boyens, NIST ITL

Team Members: Sandor Boyson, Thomas Corsi, Hart Rossman, Holly Mann, Jessica Richmond

Advisors: Taylor Wilkerson, Gary Lynch

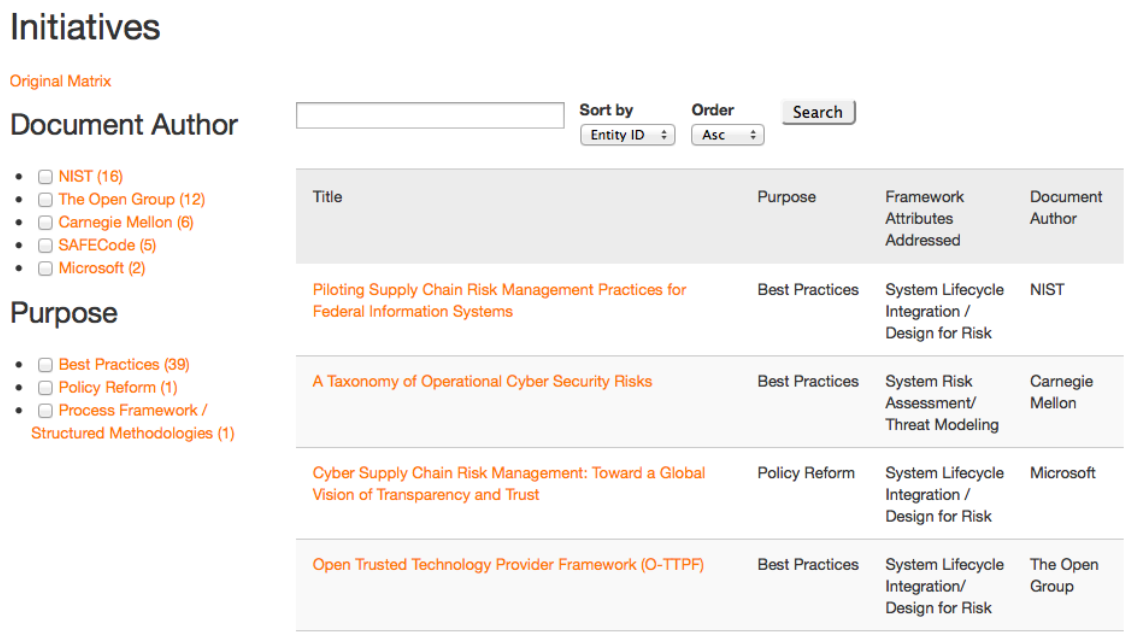
December 1, 2012

I. Executive Summary

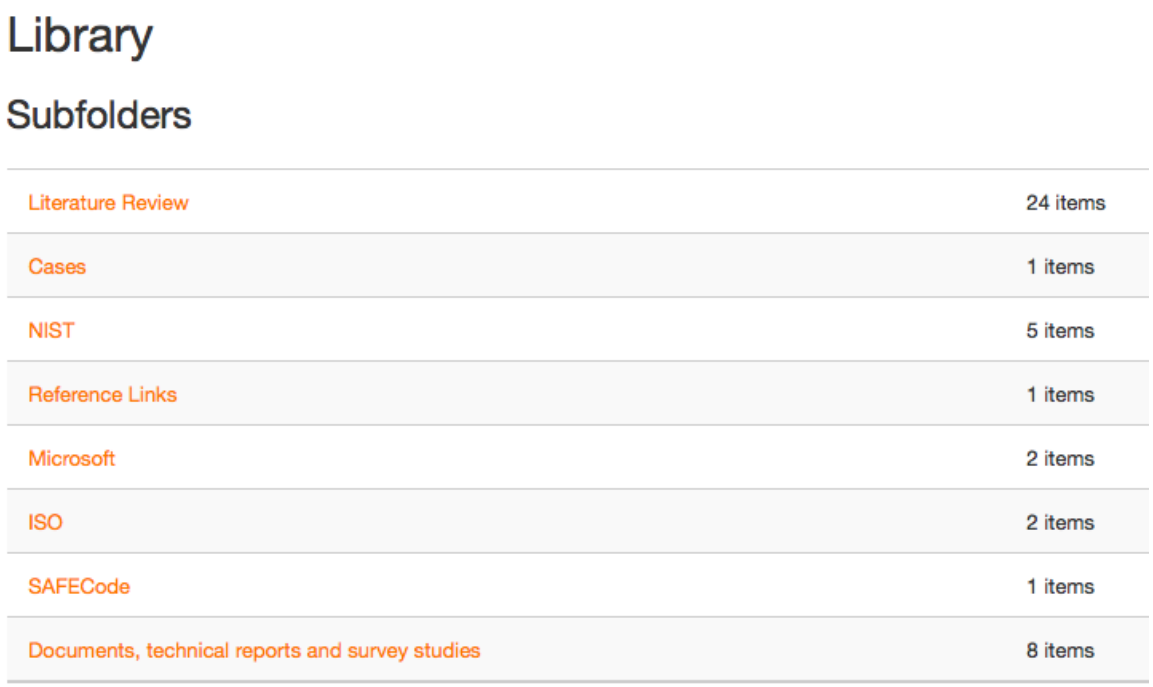
The Supply Chain Management Center of The RH Smith School Of Business, University Of Maryland has completed a third phase of research for NIST ITL built upon its prior activities; and developed an Enterprise ICT SCRM Assessment Package as a proof of concept.

This Package is delivered through an **ICT SCRM Portal**, featuring four major functions:

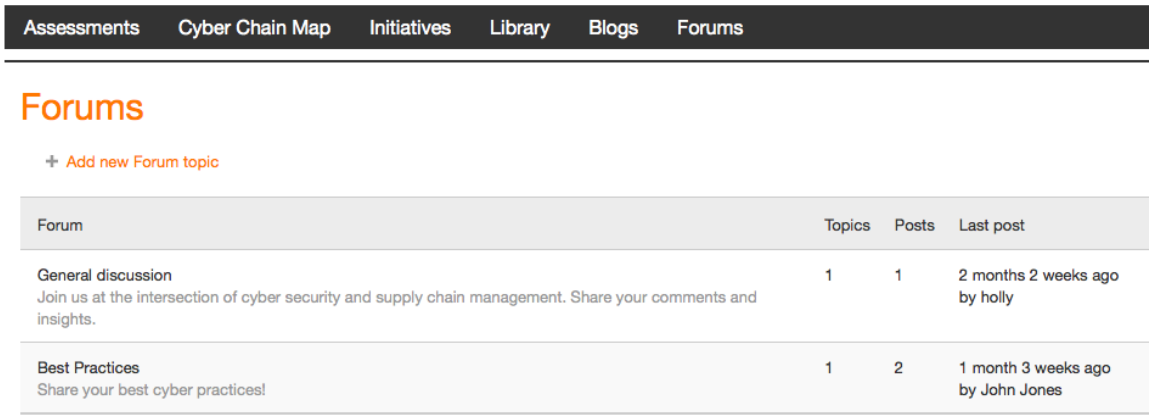
-An **Initiatives Section**, featuring upgradeable summaries of major public and private sector ICT SCRM initiatives;



-A **Library Section**, featuring a spectrum of related policy studies, case studies, research reports, etc;



-A **Forum Section** that enables collaboration groups to form around specific ICT SCRM topic areas;



-**An Enterprise Assessment Section** composed of:

-A **Strategic Readiness Tool** that profiles an enterprise's risk management posture and organizational development status.

-A **NIST Principles/Practices Tool** that drills down on the ten major principles embedded in NIST IR 7622 and asks a

portfolio of operational questions associated with each principle.

-A **Cyber Chain Mapping Tool** that provides a rapid method to build a working global map of cyber supply chain assets, transactions and vulnerabilities.

HQ

Falcon Ltd HQ

Key Hubs & Nodes

- Death Star Cloud Storage
- Mos Eisley Port
- Kessel Warehouse A
- Bespin Manufacturing

Add Node

Transactions

Falcon Ltd HQ
-> Death Star Cloud Storage

Death Star Cloud Storage
-> Bespin Manufacturing

Kessel Warehouse A
-> Mos Eisley Port

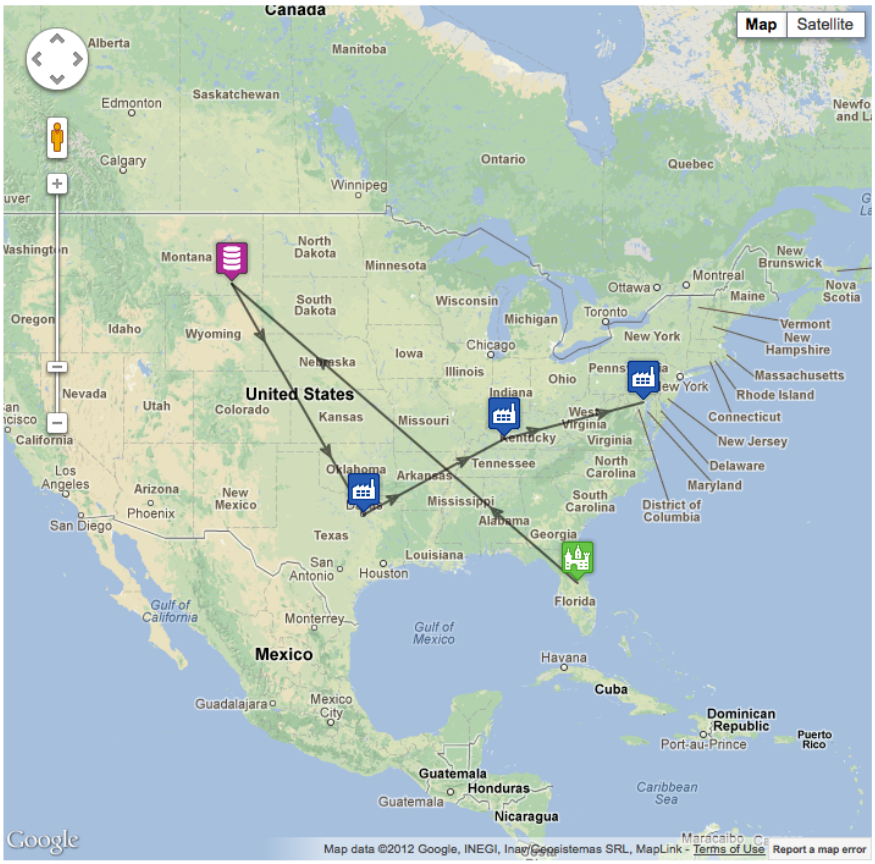
Bespin Manufacturing
-> Kessel Warehouse A

Add Transaction

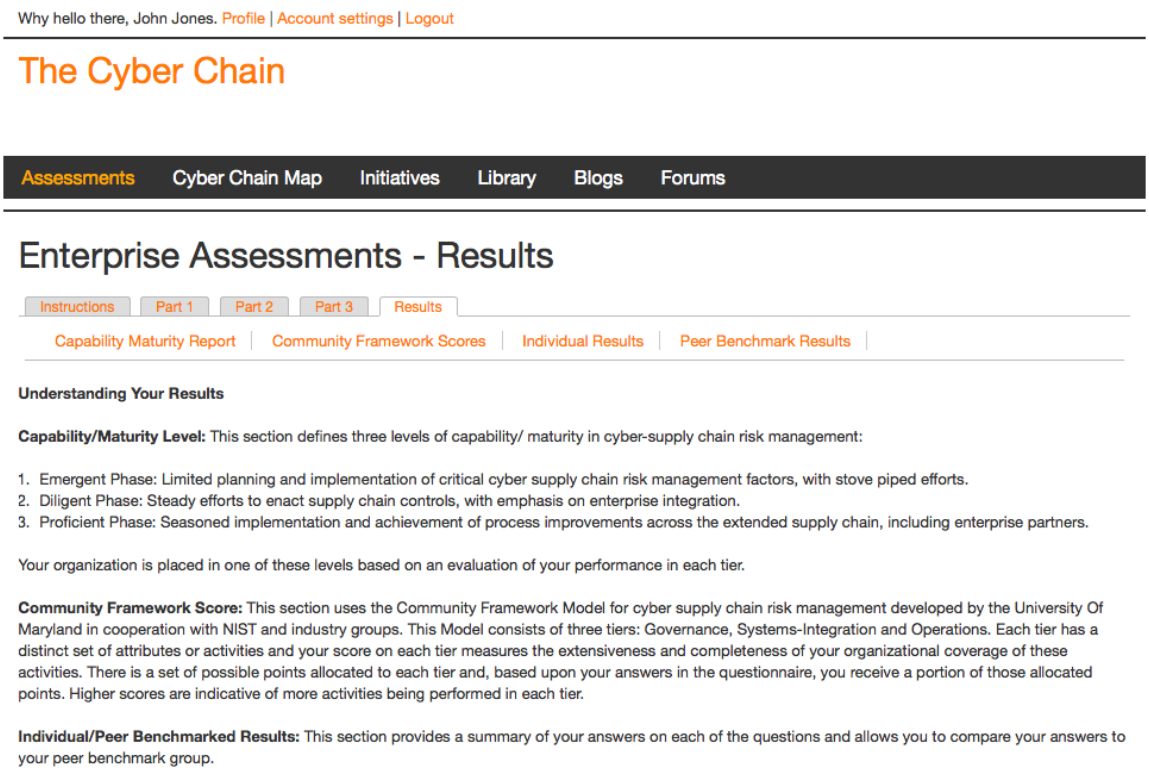
Key Actors

- Luke Skywalker
- Lando Calrissian
- Jabba T. Hutt

Supply Chain Map



-A **Results Area** that enables enterprises to view their ICT SCRM baseline status against three benchmarks: a group of peer enterprises; the Community Framework Model; and an ICT SCRM Capability/Maturity Level.



In the August-November, 2012 time period, our team accomplished all the above deliverables and presented a Portal prototype incorporating all the deliverables at the October 15-16 NIST ITL Workshop on Supply Chain Risk Management.

II. Project Highlights

Unlike previous ICT SCRM research activities undertaken by the RH Smith School Of Business for NIST, this project was engaged in the design and prototyping of a Portal that could combine a sophisticated technical architecture and advanced functionality to meet a real need for the government and private sectors.

Our team's technical activities were focused on selecting portal software that was open source and compatible with similar government initiatives. Our Smith School CIO, Ms. Holly Mann, led the effort to produce a technical architecture that was robust, secure and highly cost effective. Drupal was

selected as the software foundation for the project. Please see **Appendix 1: NIST SCRM Portal Technical Architecture** for details.

In addition, we launched a significant functionality study to understand current offerings in the marketplace; and to refine the User Interface and navigational elements of the Portal. We did a detailed comparison of existing cyber web sites and presented a wire frame of recommended Portal functional areas. This effort was led by Ms. Jessica Richmond and her background report on portal design was instrumental in our project development efforts. Please see **Appendix 2: NIST SCRM Portal Design** for details.

To complete the design process, we conducted detailed research into enterprise assessment methodologies both within and outside the ICT SCRM discipline; and sought to understand best practices in evaluating the capability/maturity levels of enterprise supply chains and cyber systems. Among the sources consulted (by area of assessment) were:

Strategic Readiness: Field visits and extended discussions were held with the Risk Group of the Security Exchange Commission; with the Executive Director of the Independent Distributors Of Electronics Association (IDEA); with the Center For Advanced Life Cycle Engineering (CALCE) University Of Maryland; and with the Principal of the Marsh Supply Chain Risk Management Practice among others.

NIST Principles/Practices: This assessment area was prepared utilizing the NIST IR 7622 as well as previous Smith research for NIST. In addition, we evaluated a variety of capability/maturity models, from the Supply Chain Council's SCOR Model to the Supply Chain Risk Leadership Council's emerging maturity criteria.

Cyber Chain Map: This assessment area was the most exploratory. It attempted to link a variety of tools such as network planning tools, Google maps and CVSS Scoring into an easy to use mapping exercise that could show both cyber as well as traditional supply chain hubs, nodes, transactions and vulnerabilities.

Field Testing The Assessment Tools: A support for our assessment development activities was the TM Forum, a twenty five year old 800 member global organization of telecommunications industry providers. This organization selectively recruited a small member pool to validate our

survey instruments and provide feedback.All efforts were made to protect the confidentiality of participant information. The survey website used SSL (secure socket layer)and HTTPS technology; and all comparative results were anonymized.

The survey was opened for a two week period starting 8am on Monday, September 17 and running through 8am on Tuesday, October 2. TM Forum participants started by going to: https://cyberchain.rhsmith.umd.edu. When the participants first landed on the main page, they saw a Register link. Since this was a closed focus group, they had to register for the site and submit a request for approval. Once approved, the system generated an email that enabled them to log onto the site and set a password. Once the assessments were completed, the Results enabled each participant enterprise to review the organization's cyber supply chain capability/maturity level; Community Framework score; and individual/as well as benchmarked results.

Three large Commercial Service Providers from North America, Australia, Europe took the survey and provided feedback. There were significant differences among respondents in many areas of ICT SCRM, as demonstrated in the table below regarding who contributes to risk management policy in each organization.

tmforum

Readiness Survey

Who contributes significantly to cyber risk management policy development?

Participant	BoD / Risk Audit Cmt	Chief Exec	Chief Financial	Chief Risk	Source / Procure	VP Supply Chain	
CSP #1	🔴	🟡	🟡	🔴	🟡	🔴	CIO
CSP #2	🟢	🟡	🟡	🟢	🟢	🟢	CIO
CSP #3	🟡	🟡	🟢	🟢	🟢	🟢	CIO

🟢 = Strong 🟡 = Moderate/Some 🔴 = Weak/Not Available

Overall, the respondents were pleased with the experience. As one noted "we have completed the Survey and found it very useful with lots of food for thought". Ms. Christy Coffey, TM Forum Program Coordinator, came to our October 16 NIST Workshop Portal Demonstrator, and presented this feedback to the workshop audience.

III. Conclusions/Recommendations

A. The Portal Concept Has Demonstrated Initial Viability

This project has demonstrated the initial viability of an open source-based ICT SCRM Portal that could provide involved federal agencies and enterprises with a best practices clearing house/website. The ICT SCRM Assessments could provide these key actors with state of the art, research-based tools to evaluate their own ICT SCRM status and improve their own Programs.

By providing a user-interface/ web-based front end and search tools, this dynamic proof-of-concept database could eventually scale to help public and private organizations:

-Search for and discover emerging ICT SCRM Practices in hardware; software; network management; and system integration

-Gain access to a Benchmarking Mechanism for evaluating effectiveness of /confidence levels in response measures that target specific threat categories across the ICT supply chain.

-Stay current with the latest Audit/Compliance/accreditation activities, including methods/issues in assessment and disclosure of risks.

-Support organizational decision making around participating in a specific external industry practice group.

-Participate in building future-forward Information-sharing models that instill transparency and confidence in ICT SCRM data exchanges among members of an industry or a supply chain:

These models could develop as *brokerage-style* concepts whereby anonymity of benchmarking data is maintained through devices such as community ratings of criticality of common components across ICT companies and ratings of effectiveness of practices matched to those levels of criticality; or as *subscription-style* concepts whereby enterprises will subscribe to alerts from a community cyber threat event/practice board.

B. The Need To Scale Up Portal Services

Any next steps should build on the existing portal platform and functionality to achieve rapid scale up and diffusion. NIST should consider scaling the portal to serve as a core component of its community-building activities in ICT SCRM; to serve as the information hub of the universe of initiatives and research resources; and to support the launch and diffusion of its key policy documents such as the NIST IR 7622 and Special Publication.

Under its own auspices or through an agreement with the Smith School, NIST has an opportunity to provide a key mechanism in advancing the ICT SCRM discipline.

A next phase of portal development might include the following activities:

-Create a Portal Advisory Group to help guide the scale up of the portal and outreach to users.

-Engage key community initiatives in updating the content of their offerings/activities in the Initiatives Section of the portal.

-Expand the Library content area of the portal.

-Deploy a network of online forums in support of NIST's ICT SCRM policy work.

-Massively expand the number of participant enterprises who complete the Enterprise Assessments; and develop a rich, segmented benchmarking repository and refined capability/maturity model.

More specifically, we would like to advance an umbrella concept that we believe captures all the key elements of a next phase in building out the NIST/University Of Maryland ICT Supply Chain Risk Management Portal. The concept is that of **an "open source" ICT Supply Chain Risk Management Technical Assistance Center that can leverage our technology infrastructure and online content for community creation purposes**.

We envision an intensive year-long project to iterate/complete the portal-based Center; to operate the portal/grow the community & demonstrate utility to a much broader audience; and to measure value.

This Center would serve as the virtual hub of the ICT supply chain risk management community and provide the following services:

-Unrestricted open access to parts of the portal, such as the Library function, that could benefit the whole community, as jointly defined with NIST.

-Screening/On Line Registration of participants for those parts of the portal, such as the Supply Chain Threat Crowdsourcing Function, that require the validation of credentials as subject matter experts, company representatives or industry practitioners through the use of layered mechanisms such as a central authentication service (CAS) and resume submissions/reviews.

-Enterprise Assessments that would enable organizations to benchmark practices in ICT SCRM against peer groups and to determine capability/maturity levels. Combined with the Map Function discussed below, a Cumulative Risk Score could be assigned to an organization.

-ICT Supply Chain Mapping and Vulnerability Analyses that would allow an organization to rapidly construct a topographical map of key physical and IT network hubs, nodes and process flows; upload data and automatically generate CVSS ratings by geographic coordinates.

-Crowd Sourced ICT Supply Chain Threat Assessment that would identify emerging threats, attack vectors, effectiveness of possible response options and contagion surveillance in real time.

-Moderated collaboration forums that would engage experts and practitioners on topics of special interest to the ICT SCRM community.

-A dynamic, continuously updating Library that would synthesize new best practices content from internal portal sources (forums, enterprise assessments, threat analyses); and external scans of professional and academic sources.

The Virtual Technical Assistance Center would produce, archive and wide cast regular material work products (monthly supply chain threat bulletins and summaries of top forum topics; quarterly report series; and synthesis of enterprise assessment/mapping data findings).

We encourage NIST to leverage the platform and toolset that has been built in this project and use them to expand its institutional connectivity and influence over the emerging discipline of ICT SCRM.

APPENDIX 1: PORTAL ARCHITECTURE

Technical Architecture Overview for Cyber Chain

The Cyber Chain website will help organizations prepare for global cyber supply chain challenges through utilizing the online tools, resources and assessments available in this site. This document includes a summary of technical approach and components used to develop this site.

Framework Approach

The decision to build the site using an ope source application (Drupal) provides the following benefits:

- No licensing fees or contractual obligations.
- No proprietary "black box." This means that everything in the Drupal framework is transparent to a programmer with the knowledge to look at the source code.
- Drupal has been an active open source application for over 10 years. It is a mature application that has been adopted and used by thousands of developers. These developers contribute custom built modules that can be leveraged the Drupal community, at no cost.
- Compatibility with external applications and databases are essential. PHP and MySQL will be utilized for additional program code and common data store.
- Persistent design techniques are applied using this platform. This means the site will automatically adapt for usage with mobile devices. The user experience will be exactly the same without the need to maintain a separate mobile site.
- Password security in the Drupal framework is in compliance with government agencies. A dedicated Drupal security team reviews all submitted modules for security compliance and does not publish those with unresolved security issues. We will utilize SSL certificates, as well as, an administrative approval process to gain access to this site. The data contained in

Basic Server Configuration

- Virtual Machine
- HTTPS/SSL connections
- Operating System: CentOS 6.x
- Web Server: Apache 2.x
- Database Server: MySQL 4.x
- PHP 5.x
- Drupal 7

Drupal Modules

this site will not be visible to anyone other than the authorized person utilizing the tools or administering the site.

- The site will be hosted at the University of Maryland, Robert H. Smith School of Business, unless otherwise specified in agreement between RHS and NIST.

Site Content

TA 1 – ASSESSMENTS

Thi tab contains fou sub tabs 1 Respondent Profile, 2 Strategic Readines Survey 3 NIST Principles/Practices, an 4 Results.

1. **Registration/Profile** – the site requires registration for a login account to obtain access to the tools and resources. All registration requests will be reviewed and approved by a system administrator. A respondent profile is created for each authorized account. The information contained in this profile provides the foundation for individual and peer benchmarked results.

2. **Strategic Readiness Survey –** will be completed by the authorized user and serves as the basis to access the structural readiness of their organization to meet the challenges of cyber supply chain risk management**.**

3. **NIST Principles/Practices** – are designed to distill best practices developed by NIST into a series of specific questions about their operating practices.

4. **Results** - once the authorized user has completed ALL of the assessment parts, this tab will be displayed. This tab contains four sub tabs a) Capability/Maturity Level, b) Community Framework Score, c) Individual Results, d) Peer Benchmark Results

    a) **Capability/Maturity Level:** This section defines three levels of capability/ maturity in cyber-supply chain risk management:

    - Emergent Phase: Limited planning and implementation of critical cyber supply chain risk management factors, with stove piped efforts.
    - Diligent Phase: Steady efforts to enact supply chain controls, with emphasis on enterprise integration.

ASSESSMENT FUNCTIONS

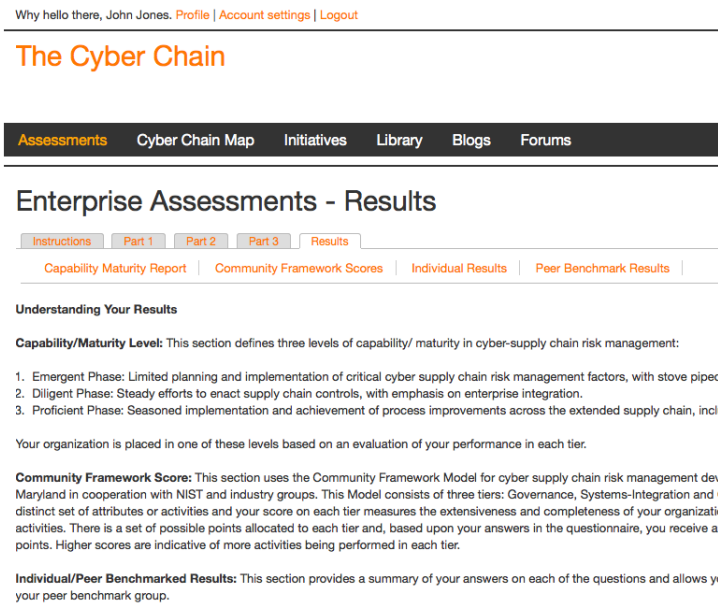
- Users must complete the assessments in sequence.
- New assessments and sub tabs will become visible only upon completion of each.
- Users have the ability to save the submission As Draft, allowing them to return later to edit and submit the final assessment.
- Users may view their individual submissions however they cannot edit their submissions once final responses have been submitted.
- Results for capability maturity and community framework are derived through a set of complex formulas based on a point system.

- Proficient Phase: Seasoned implementation and achievement of process improvements across the extended supply chain, including enterprise partners.

Your organization is placed in one of these levels based on an evaluation of your performance in each tier.

b) **Community Framework Score:** This section uses the Community Framework Model for cyber supply chain risk management developed by the University Of Maryland in cooperation with NIST and industry groups. This Model consists of three tiers: Governance, Systems-Integration and Operations. Each tier has a distinct set of attributes or activities and your score on each tier measures the extensiveness and completeness of your organizational coverage of these activities. There is a set of possible points allocated to each tier and, based upon your assessment responses you receive a portion of those allocated points. Higher scores are indicative of more activities being performed in each tier.

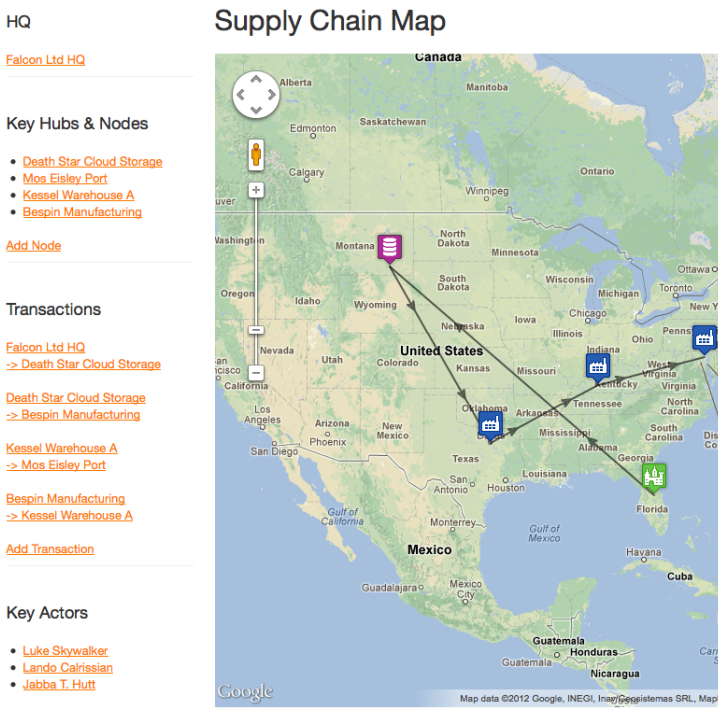
c) **Individual/Peer Benchmarked Results:** This section provides a summary of your answers on each of the questions and allows you to compare your answers to your peer benchmark group.



TAB 2 – CYBER CHAIN MAP

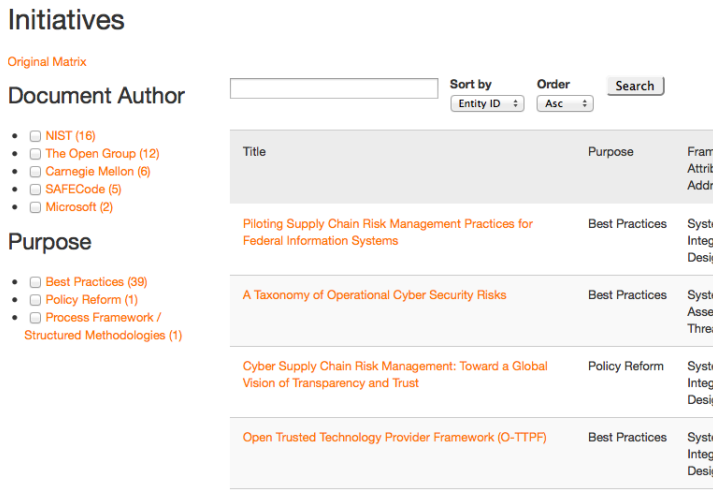
This tab contains a composite network vulnerability mapping exercise. This tool will

allow users to setup supply chain risk scenarios. The composite system will generate and execute the components for each scenario, composes the risk data, defines the threats and overall risk assessment.



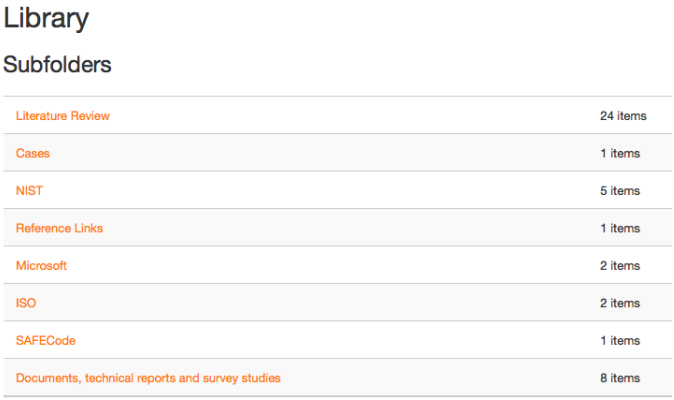
TAB 3 – INITIATIVES

This tab contains a viewable link to the original detailed matrix of ICT SCM initiatives. In addition, each initiative is prepared as individual content in order to allow the users to conduct a full text search to locate specific initiatives that meet their search criteria. The ICT SCM initiatives categorized by document author, and purpose.



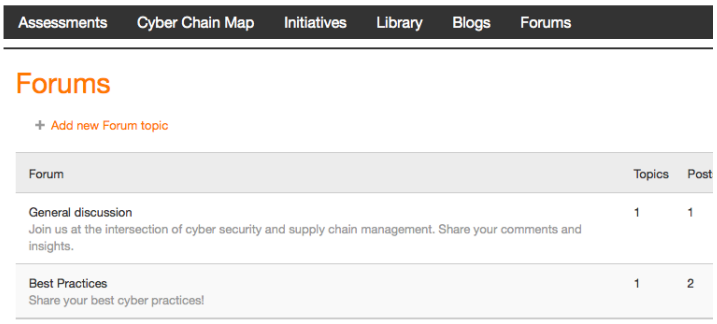
TAB 4 – LIBRARY

This tab contains a document repository of research papers, case studies, and reports on ICT SCM related materials. Users can create their own folders and upload related ICT SCM related documents for the cyber chain community.



TAB 5 – FORUMS

This tab consists of four major components: the forum itself, categories, topics and messages. Users can create new forum categories, and reply to messages that will appear as a threaded conversation. Users will see the number of topics and responses posted within each category, and the date/time/author of the posts.


Assessments
Cyber Chain Map
Initiatives
Library
Blogs
Forums
Forums
+ Add new Forum topic
Forum
Topics
Post
General discussion
Join us at the intersection of cyber security and supply chain management. Share your comments and insights.
1
1
Best Practices
Share your best cyber practices!
1
2