Current Awareness of the Cybersecurity Framework

1. What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

Answer: I can only speak for myself and the answer would be two counts of yes. I was able to bring this to the attention of senior leadership while being employed by DynCorp International, one of the Top Defense Contractors where we transitioned to a hybrid NIST 800-53 and Cybersecurity framework. The second account is my current employer HD Vest Financial Services within the Financial Sector. This framework was not known prior to my hire back in July 2014.

2. How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?

Answer: Coming out of the United States Air Force and working as a contractor within the Drug Enforcement Administration's Aviation Division I have always been knowledgeable on NIST and its actions. It was also briefly mentioned in topic a few times at EC-Council's Global CISO Forum held in Atlanta, GA during Hacker Halted.

3. Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?

Answer: I have personally mentioned the framework in topic during several interviews with Abmit Energy within the energy sector and Neiman Marcus within the retail sector. Additionally similar questions are being asked by the U.S. Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and the Securities Industry and Financial Markets Association (SIFMA).

4. Is there general awareness that the Framework:

a. Is intended for voluntary use?

Answer: Yes

b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?

Answer: Yes but some pushback has existed with how risk is currently being performed and the levels and tiers.

c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?

Answer: Yes, it was mentioned this is a living document.

5. What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?

Answer: Getting into the conversation within the leadership level of the company. There is tremendous opportunity for business growth. My recommendation is to add two additional elements to each individual control one called rating and one called priority. The priority is from a business's point of view and just about anything you do on a daily basis can be placed into one of these three areas. This allows the public and private sector to flex the framework to fit their business needs. Table 1 and 2 are provided below for reference to the ratings and rankings followed by Table 3 will shows the control assessment results summary by NIST Cybersecurity family; Tables 4 shows the control assessment results summary by NIST Cybersecurity control family to business priority; Table 5 shows the summary of NIST Cybersecurity controls assessed for a particular quarter. The data is not real just for educational purposes. Table 6 shows what an individual control might look like.

Table 1: Business Priority Rankings

	Priority	Description
1	**Break/Fix**	Keep internal and external customers operational Controls View: Immediate action required
2	**Growth Impacting**	Pursuit of new business/growth or cost savings opportunity Controls View: Further action is necessary
3	**Routine**	Sustainment and maintenance of current environment Controls View: Functional and operational, consider more
4	**Innovation**	What to do versus must do, the good ideas Controls View: Above and beyond, excellence

Table 2: Individual Control Ratings

	Priority	Description
1	**High or Insufficient**	A material weakness with a control design or execution has been discovered, a corrective action plan is needed or a risk acceptance form needs endorsed by a member of executive leadership.
2	**Medium or Marginal**	Discrepancies were discovered in the control testing however does not present a major organizational risk or weakness, further testing may be required
3	**Low or Sufficient**	The control is operating within the acceptable parameters, no further action is necessary.

Table 3: Control assessment results summary by NIST Cybersecurity control family

Control Family	Insufficient	Marginal	Sufficient	Total
Identify – Asset Management	🟥	🟨	🟩	**6**
Identify – Business Environment	🟥	🟨	🟩	**5**

Identify – Governance	🟥	🟨	🟩	4
Identify – Risk Assessment	🟥	🟨	🟩	6
Identify – Risk Management Strategy	🟥	🟨	🟩	3
Protect – Access Control	🟥	🟨	🟩	5
Protect – Awareness and Training	🟥	🟨	🟩	5
Protect – Data Security	🟥	🟨	🟩	7
Protect – Information Protection Processes and Procedures	🟥	🟨	🟩	12
Protect – Maintenance	🟥	🟨	🟩	2
Protect – Protective Technology	🟥	🟨	🟩	4
Detect – Anomalies and Events	🟥	🟨	🟩	5
Detect – Security Continuous Monitoring	🟥	🟨	🟩	8
Detect – Detection Processes	🟥	🟨	🟩	5
Respond – Response Planning	🟥	🟨	🟩	1
Respond – Communications	🟥	🟨	🟩	5
Respond – Analysis	🟥	🟨	🟩	4
Respond – Mitigation	🟥	🟨	🟩	3
Respond – Improvements	🟥	🟨	🟩	2
Recover – Recovery Planning	🟥	🟨	🟩	1
Recover – Improvements	🟥	🟨	🟩	2
Recover – Communications	🟥	🟨	🟩	3
Totals	🟥	🟨	🟩	98

Table 4: Control assessment results summary by NIST Cybersecurity control family to business priority

Control Family	Priority 1	Priority 2	Priority 3	Priority 4	Total
Identify – Asset Management	🟥	🟩	🟦	🟪	6
Identify – Business Environment	🟥	🟩	🟦	🟪	5
Identify – Governance	🟥	🟩	🟦	🟪	4
Identify – Risk Assessment	🟥	🟩	🟦	🟪	6
Identify – Risk Management Strategy	🟥	🟩	🟦	🟪	3
Protect – Access Control	🟥	🟩	🟦	🟪	5
Protect – Awareness and Training	🟥	🟩	🟦	🟪	5
Protect – Data Security	🟥	🟩	🟦	🟪	7
Protect – Information Protection Processes and Procedures	🟥	🟩	🟦	🟪	12
Protect – Maintenance	🟥	🟩	🟦	🟪	2
Protect – Protective Technology	🟥	🟩	🟦	🟪	4
Detect – Anomalies and Events	🟥	🟩	🟦	🟪	5
Detect – Security Continuous Monitoring	🟥	🟩	🟦	🟪	8
Detect – Detection Processes	🟥	🟩	🟦	🟪	5
Respond – Response Planning	🟥	🟩	🟦	🟪	1
Respond – Communications	🟥	🟩	🟦	🟪	5
Respond – Analysis	🟥	🟩	🟦	🟪	4
Respond – Mitigation	🟥	🟩	🟦	🟪	3

Respond – Improvements	🟥	🟩	🟦	🟪	**2**
Recover – Recovery Planning	🟥	🟩	🟦	🟪	**1**
Recover – Improvements	🟥	🟩	🟦	🟪	**2**
Recover – Communications	🟥	🟩	🟦	🟪	**3**
Totals					**98**

Table 5: Summary of NIST Cybersecurity controls assessed for a particular quarter.

Control	Control Family	Score	Priority	Function
ID.AM-1	**Asset Management**	🟨	🟥	**Identify**
ID.AM-2	**Asset Management**	🟨	🟥	**Identify**
ID.AM-3	**Asset Management**	🟨	🟩	**Identify**
ID.AM-4	**Asset Management**	🟥	🟥	**Identify**
ID.AM-5	**Asset Management**	🟩	🟩	**Identify**
ID.AM-6	**Asset Management**	🟩	🟩	**Identify**
ID.BE-1	**Business Environment**	🟨	🟩	**Identify**
ID.BE-2	**Business Environment**	🟩	🟪	**Identify**
ID.BE-3	**Business Environment**	🟩	🟦	**Identify**
ID.BE-4	**Business Environment**	🟨	🟥	**Identify**
ID.BE-5	**Business Environment**	🟩	🟦	**Identify**
ID.GV-1	**Governance**	🟩	🟦	**Identify**
ID.GV-2	**Governance**	🟨	🟩	**Identify**
ID.GV-3	**Governance**	🟩	🟩	**Identify**
ID.GV-4	**Governance**	🟨	🟦	**Identify**
ID.RA-1	**Risk Assessment**	🟥	🟥	**Identify**
ID.RA-2	**Risk Assessment**	🟨	🟩	**Identify**
ID.RA-3	**Risk Assessment**	🟩	🟩	**Identify**
ID.RA-4	**Risk Assessment**	🟩	🟥	**Identify**
ID.RA-5	**Risk Assessment**	🟩	🟪	**Identify**
ID.RA-6	**Risk Assessment**	🟩	🟪	**Identify**
ID.RM-1	**Risk Management Strategy**	🟩	🟦	**Identify**
ID.RM-2	**Risk Management Strategy**	🟩	🟪	**Identify**
ID.RM-3	**Risk Management Strategy**	🟩	🟩	**Identify**
PR.AC-1	**Access Control**	🟥	🟩	**Protect**
PR.AC-2	**Access Control**	🟩	🟪	**Protect**
PR.AC-3	**Access Control**	🟨	🟩	**Protect**
PR.AC-4	**Access Control**	🟥	🟩	**Protect**
PR.AC-5	**Access Control**	🟩	🟥	**Protect**
PR.AT-1	**Awareness and Training**	🟩	🟥	**Protect**
PR.AT-2	**Awareness and Training**	🟩	🟪	**Protect**
PR.AT-3	**Awareness and Training**	🟩	🟦	**Protect**
PR.AT-4	**Awareness and Training**	🟩	🟩	**Protect**
PR.AT-5	**Awareness and Training**	🟨	🟦	**Protect**

PR.DS-1	Data Security	🟩	🟦	Protect
PR.DS-2	Data Security	🟨	🟦	Protect
PR.DS-3	Data Security	🟥	🟥	Protect
PR.DS-4	Data Security	🟩	🟩	Protect
PR.DS-5	Data Security	🟥	🟥	Protect
PR.DS-6	Data Security	🟥	🟥	Protect
PR.DS-7	Data Security	🟨	🟦	Protect
PR.IP-1	Information Protection Process and Procedures	🟩	🟥	Protect
PR.IP-2	Information Protection Process and Procedures	🟩	🟦	Protect
PR.IP-3	Information Protection Process and Procedures	🟨	🟪	Protect
PR.IP-4	Information Protection Process and Procedures	🟩	🟦	Protect
PR.IP-5	Information Protection Process and Procedures	🟩	🟦	Protect
PR.IP-6	Information Protection Process and Procedures	🟩	🟦	Protect
PR.IP-7	Information Protection Process and Procedures	🟩	🟪	Protect
PR.IP-8	Information Protection Process and Procedures	🟥	🟥	Protect
PR.IP-9	Information Protection Process and Procedures	🟨	🟩	Protect
PR.IP-10	Information Protection Process and Procedures	🟩	🟦	Protect
PR.IP-11	Information Protection Process and Procedures	🟩	🟩	Protect
PR.IP-12	Information Protection Process and Procedures	🟩	🟥	Protect
PR.MA-1	Maintenance	🟨	🟦	Protect
PR.MA-2	Maintenance	🟩	🟦	Protect
PR.PT-1	Protective Technology	🟨	🟦	Protect
PR.PT-2	Protective Technology	🟩	🟥	Protect
PR.PT-3	Protective Technology	🟩	🟪	Protect
PR.PT-4	Protective Technology	🟩	🟥	Protect
DE.AE-1	Anomalies and Events	🟥	🟥	Detect
DE.AE-2	Anomalies and Events	🟨	🟦	Detect
DE.AE-3	Anomalies and Events	🟨	🟩	Detect
DE.AE-4	Anomalies and Events	🟥	🟦	Detect
DE.AE-5	Anomalies and Events	🟩	🟩	Detect
DE.CM-1	Security Continuous Monitoring	🟩	🟥	Detect
DE.CM-2	Security Continuous Monitoring	🟩	🟦	Detect

DE.CM-3	Security Continuous Monitoring	🟩	🟦	Detect
DE.CM-4	Security Continuous Monitoring	🟨	🟥	Detect
DE.CM-5	Security Continuous Monitoring	🟥	🟩	Detect
DE.CM-6	Security Continuous Monitoring	🟨	🟪	Detect
DE.CM-7	Security Continuous Monitoring	🟩	🟥	Detect
DE.CM-8	Security Continuous Monitoring	🟩	🟥	Detect
DE.DP-1	Detection Processes	🟩	🟦	Detect
DE.DP-2	Detection Processes	🟩	🟦	Detect
DE.DP-3	Detection Processes	🟩	🟪	Detect
DE.DP-4	Detection Processes	🟩	🟦	Detect
DE.DP-5	Detection Processes	🟥	🟪	Detect
RS.RP-1	Response Planning	🟨	🟥	Respond
RS.CO-1	Communications	🟥	🟩	Respond
RS.CO-2	Communications	🟩	🟦	Respond
RS.CO-3	Communications	🟩	🟦	Respond
RS.CO-4	Communications	🟩	🟦	Respond
RS.CO-5	Communications	🟩	🟪	Respond
RS.AN-1	Analysis	🟨	🟦	Respond
RS.AN-2	Analysis	🟩	🟩	Respond
RS.AN-3	Analysis	🟩	🟥	Respond
RS.AN-4	Analysis	🟩	🟦	Respond
RS.MI-1	Mitigation	🟩	🟦	Respond
RS.MI-2	Mitigation	🟩	🟥	Respond
RS.MI-3	Mitigation	🟩	🟥	Respond
RS.IM-1	Improvements	🟩	🟪	Respond
RS.IM-2	Improvements	🟨	🟦	Respond
RC.RP-1	Recovery Planning	🟥	🟦	Recover
RC.IM-1	Improvements	🟨	🟪	Recover
RC.IM-2	Improvements	🟩	🟦	Recover
RC.CO-1	Communications	🟥	🟥	Recover
RC.CO-2	Communications	🟨	🟥	Recover
RC.CO-3	Communications	🟩	🟩	Recover

Table 6: Example of a control within an assessment.

RS.CO-5 Response Communications	
Control	Rating
Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	🟥

[Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies]	🟥
Assessment	
Information is only shared with federal agencies. Information is not disseminated to the public, external stakeholders or industry members.	
Recommendation	
Law enforcement and other members of the energy industry should be kept informed on cyber activities by sharing information. The public should be kept up to date on what the company is doing on a proactive basis to minimize customer perception and confidence in the event of an incident.	
Management's Comments	

Priority
4

Notice this is a business priority 4. Something that has a higher business priority would be worked first in this case since the overall rating for this control is red, which means high or insufficient. Another control that has an overall rating of yellow, which means medium or marginal and has a business priority of a 1 which means break fix would probably take precedence over the above control even through the individual control is rated worse, but the business priority is innovation.

6. Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?

Answer: Coming from a previous Defense Contractor operating in remote parts of the world I know there is awareness of the framework at a very high level with those performing information security functions; however I do not know if the business units operating in the remote parts are aware of the framework.

7. If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?

Answer: Yes the Securities and Exchange Commission (SEC), Financial Industry Regulatory Autority (FINRA) and the Securities Industry and Financial Markets Association (SIFMA) are all aware as they have all released communications indicating they would be examining several firms for content within the framework and mention it in the communication.

8. Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?

Answer: Yes the current Risk Management team is only aware the framework exists but they do not know how it impacts the business nor do they understand the functions within the framework. I have personally started educating some of the Risk Management team on the concept of the framework and its importance. There is some resistance of implementing or identifying a new framework because it brings new gaps that need to be addressed and requires a change in how the business is currently operating in relation to other frameworks not within cybersecurity.

9. What more can and should be done to raise awareness?

Answer: There needs to be collaboration amongst the various sectors identified within the critical infrastructure and the holding of events to bring credibility to the framework and its importance for businesses to take it seriously. Being a Chief Information Security Officer in addition to being a finalist for the 2013 and 2014 Certified Chief Information Security Officer of the Year Award presented by EC-Council I still find it an uphill battle to get the business onboard with security related issues not to mention changing or implementing frameworks to identify gaps. If the same information I was communicating to the business was also communicated at national and global levels (conference, summits, etc.) where they can attend and see a holistical view of multiple sectors talking about the same thing I believe the business would be less resistant to change.

Experiences with the Cybersecurity Framework

1. Has the Framework helped organizations understand the importance of managing cyber risk?

> *Answer: I do not believe this has since there has been resistance from within the Risk Management departments and the validity of the data obtained during the framework assessment. For instance I recently conducted an assessment but had to caveat on all the documentation that it was not validated by the Risk Management department.*

2. Which sectors and organizations are actively planning to, or already are, using the Framework, and how?Show citation box

> *Answer: Financial Services Sector of the Critical Infrastructure to include smaller broker-dealer firms since the SEC, FINRA, and SIFMA are already conducting assessments on the criteria.*

3. What benefits have been realized by early experiences with the Framework?

> *Answer: The framework has wiggle room to fit each business. I mapped the framework to all the controls in NIST 800-53 v4 as well as the additional supplemental Privacy and Project Management controls and the SANs Top 20 Critical controls. I then gave each of them a base number and multipliers based on their importance, determined their density based on the number of times mentioned as a primary or supporting control and what they can do technically and move the needle (The excel spreadsheet is available upon request if you would like to see it). This allows the business to flex as the framework control descriptions are left to a subjective view.*

4. What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?

> *Answer: The controls within the framework need clarification sort of like how NIST 800-53 has for each control. Without this the control is wide open to interpretation and is completely a subjective view by the Information Security department, the Risk Management department and Internal Audit.*

5. Do organizations in some sectors require some type of sector specific guidance prior to use?

> *Answer: The financial services sector and the SEC seem to have some frameworks already established and identified and the Cybersecurity framework uses different terminology for risk. For instance a High rating in the framework is insufficient in the SEC frameworks for identifying control risks.*

6. Have organizations that are using the Framework integrated it with their broader enterprise risk management program?

> *Answer: There has been no integration to date.*

7. Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?

> *Answer: The one item that I have found to be a stump with the business is the implementation tiers. The business I thinking of these as maturity. I would consider either adding maturity to the existing framework since these are not always in alignment with one another.*

8. Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.

a. Of these recommended practices, how are organizations initially using the Framework?

> *Answer: The framework is being used as a talking point but due to a lack of regulatory requirement to use the framework it is not gaining the traction needed.*

b. Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?

> *Answer: I think some Information Security departments are using it as a supporting document to whatever existing frameworks they are using if any.*

c. Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?

> *Answer: I believe this is best effort as most businesses I have had the opportunity to work with are operating very lean which means budgets are tight and the stakeholders and board members want to keep costs down. Information Security doesn't have a direct cost savings other than cost avoidance in most cases so it is a hard sell to get them onboard to address these areas in a proactive manner. Cyber insurance is being used as a safety net in most cases.*

d. Are organizations changing their cybersecurity governance as a result of the Framework?

> *Answer: I do not believe so since there is still resistance with the Risk Management and Internal Audit departments.*

e. Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?

> *Answer: There have been several attempts however the cost of security is not seen as an investment. There is no direct cost savings tied to most initiatives so the Cyber insurance is an easy safety net as mentioned above.*

f. Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?

Answer: There are some items within the framework that have already been in place for assessing risk with vendors through security assessments but nothing directly identifying the framework.

9. Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?

Answer: National as well as Regional conferences need to be established where those agencies are in attendance if not presenters along with other sectors within the critical infrastructure. Information Security departments I believe are onboard it is the rest of the business that needs to be brought onboard and that is only going to be done through collaboration and buy in from everyone across multiple industries.

10. Have organizations developed practices to assist in use of the Framework?

Answer: There are current awareness activities in place to bring education of the framework to be business in hopes the framework is identified for use and practices.

Roadmap for the Future of the Cybersecurity Framework

1. Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?Show citation box

> *Answer: I believe so; however there needs to be an industry standard business prioritization matrix as I mentioned in my above examples. Having a particular number of controls rated as high or even medium may be too much for a business to overcome and be reluctant to stick with the framework. The business priority matrix allows for each business to identify each control in the framework independently to their business. A control that is routine for one might be innovation for another.*

2. Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?

> *Answer: There is one significant issue in my opinion regarding the framework. There needs to be more around Operations and having a skilled (engineers versus analysts) and qualified cybersecurity staff focused on operations. All of the controls inside the framework are dependent upon having those staff in place. Otherwise security will always be a secondary function for most businesses.*

3. Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?

> *Answer: I mentioned something I found useful above and gave examples. I would be more than happy to provide a raw template.*