National Institute of Standards and Technology RFI

RFI Document Citation: 78 FR 13024

National Institute of Standards and Technology RFI

A Response from RSA

Presented to:

Diane Honeycutt

National Institute of Standards and Technology

100 Bureau Drive, Stop 8930

Gaithersburg, MD 20899

Presented By:

John McCumber

Federal Technologist

703 889 8950

john.mccumber@rsa.com

Cover Letter

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Attention: Diane Honeycutt

Reference: Cybersecurity Framework RFI

Dear Ms Honeycutt,

On behalf of EMC and RSA, The Security Division of EMC, we are pleased to submit our responses to the NIST request for information: Developing a Framework to Improve Critical Infrastructure Cybersecurity. Our response and comments provide an exceptional combination of real-world experience, innovative technology, and unrivalled subject matter expertise that can guide and inform your critical infrastructure initiative. It has been our pleasure to gather these processes and capabilities into a comprehensive document to address each of your questions with solid know-how from decades in the information technology realm as a vendor, solution provider, and a consumer of leading edge information technology.

RSA/EMC has unique insights to share. We are the leader in security management that allows public and private sector organizations to build and invest in information security from a rational and strategic perspective. Not only do we build the key components for continuous monitoring, digital forensics, incident response, and governance, we also have developed a set of solutions that address the key pain points of disconnected safeguard technologies. Our professional services teams are currently helping hundreds of organizations design and implement world class operational security solutions.

Our EMC/RSA response focuses on the elements of both preventive capabilities as well as the necessity for remedial/ongoing response and risk mitigation. As technology leaders in this vital market, we recognize security cannot be defined as a state; security must be defined as a process. Security is the ongoing management of risk through the identification of threats, vulnerabilities and assets weighed against the capabilities of a plethora of safeguards. It's no longer sufficient to perform security engineering solely as a static, preventive activity. Dynamic risk management capabilities are required to respond to existing and emerging threats.

Ensuring the new framework dovetails and supports international standards will be critical. The IETF efforts on security automation are critical to gaining global acceptance on protocols and data formats. As security automation improves, control frameworks can be used to manage security requirements and reporting across and between multinational organizations and governments as well. This combination of consistent reporting on automated controls will only increase in importance as use of cloud computing environments expands.

As NIST builds its new framework for protecting our critical digital infrastructure, there will be many challenges in order to maintain currency with the emerging threat landscape. EMC/RSA stands ready to support NIST's efforts to protect the citizens and institutions of our nation. If you require any further information or clarification of any elements of our response, please feel free to contact me directly at any time at john.mccumber@rsa.com, or call me at (919) 522-0084.

Sincerely,

John McCumber

RSA Federal

10700 Parkridge Boulevard

Trademark & Copyright Notices

EMC Corporation Trademarks

This is a current listing of trademarks owned by EMC Corporation. The status column refers to the status of the trademark in the United States. Not all common law marks used by EMC Corporation are listed: http://www.emc.com/legal/emc-corporation-trademarks.htm

Copyright

RSA Contacts and Document Information

Document Information		
Document title:	National Institute of Standards and Technology A Proposal from RSA	
Customer Reference	Document Citation 78 FR 13024	
Issue date:	Monday, April 08, 2013	
Submitted to:	National Institute of Standards and Technology 100 Bureau Drive, Stop 8930 Gaithersburg, MD 20899	
Account Team		
RSA Account Manager	John McCumber	Phone: 919 522 0084 Email: john.mccumber@rsa.com
EMC Corporate Office of CTO	Kathleen Moriarty	Phone: 617 583 0846 Email: kathleen.moriarty@emc.com
RSA Proposal Manager	Melissa Ferguson Meo	Phone: 1 781 515 5249 Email: melissa.meo@rsa.com

Table of Contents

1 Our Response to Your Specific RFI Requirements

This section of our proposal outlines the key functionality and other important features of the proposed solution in the context of NIST's stated requirements. Specifically, it provides a clause-by-clause response to your RFI – for ease of evaluation, each of your questions has been re-stated in normal black type, with our responses highlighted using *blue italics*.

1.1 Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

The top concern today for most organizations is how to combat complex advanced and targeted attacks. A majority of investigated cases related to data leakage, financial loss, advanced threats, or other network breach involve some form of undetected malicious executable (e.g., customizable commercial malware or "designer malware") that has been used to maintain a foothold into compromised networks. Social engineering, phishing attacks, malware, and system or application vulnerabilities are leveraged to gain or increase access within organizations. Recent trends in attacks also exploit the supply chain to gain access within an organization, creating a complex web to detect and combat threats. Obfuscation techniques are evolving at an increasing rate and traditional security tools cannot keep up. The current threat environment demands a fresh, agile approach to

1. Ensure the security of software applications in the supply chain,

2. Automate the ability to identify, prioritize, and remediate risk based on situational awareness for decision support

3. Targeted capabilities for the identification and analysis of malware or other host based threats, network based threats, and fraud detection.

4. Share meaningful, directed, and actionable information in a machine consumable way. This may be through sharing partnerships as well as from vetted vendor threat feeds for a broad, scalable, and more immediate impact for both large and small organizations.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

Creating a successful cross-sector standards-based framework for critical infrastructure will present several challenges. The first challenge will be to determine commonalities between sectors that can be

used to define the areas that will be covered in a central framework. The next challenge will be in selecting the appropriate sets of International standards that meet the core needs of all sectors and are both flexible and extensible to accommodate extensions for industry specific needs. In addition to having a flexible framework that can be updated over time, the selected International standards will need to be updated over time, ideally in standards bodies supported by the core user bases or problem owners. The framework will also need to be scalable to accommodate both small and large organizations within each sector where resource availability will greatly vary. The flexibility and extensibility of the selected standards should be helpful to support the varying needs for each sector, with a need for increased automation to assist with resource constraints for IT Security experts. Another challenge will be to have a standard method of measuring compliance to global standard frameworks rather than individual requirements of individual policy requirements, regulations, customers in the supply chain, and sectors to governments.

As information sharing becomes more pervasive, it will be a great challenge to ensure the data exchanged is meaningful, directed, and actionable. We have made great progress in some of today's sharing circles, but will need to shift the sharing models to interchange data gathered with threat feed providers who can further vet data and supply it in quick and actionable ways, reducing the overall need for highly skilled resources at each organization. If a larger ecosystem is not included in the framework, the current resource constraints and ability to implement controls for shared threat data will not improve.

And finally, cross sector communications present a challenge to determine what is actually useful and meaningful to exchange between sectors. In some cases, high-level strategic information will be far more useful than specific cyber threat remediation information. A simple example may include the energy sector loosing power in a region. Although it may have been the result of a cyber attack, the useful information to be shared cross-sector may be where the power outage occurred, what backup measures are available, and an estimated time to recover. Determining what is useful will take time and will require flexible and extensible standards to accommodate the evolving set of exchanges.

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

RSA and EMC use our own technology to manage our risk exposure on a 24x7x365 basis. Cyber security risk is specifically derived and overseen by the EMC Global Security organization in conjunction with an Enterprise Governance Risk and Compliance (eGRC) board made up of corporate executives across all major divisions of the company.

4. Where do organizations locate their cybersecurity risk management program/office?

The cybersecurity risk management office is located within the EMC IT organization but cyber risk is also elevated as need to the eGRC as described above and the Chief Risk Officer that ties into EMC Legal.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

We do not currently have an explicit enterprise risk taxonomy. Within cyber security, we use multiple factors to assess impact (Is the asset considered important to Brand?, Will there be a regulatory impact?, Is it important to the overall continuity of operations and the ability to provide order fulfillment?, Would it impact the corporate customer base directly?, Is there risk to intellectual property that would impact competitive advantage?, Would any of the risks be combined with an impact that is limited to a

single BU, multiple BUs, or is the risk enterprise wide?), and probability (Is there an active threat in the wild or not?, What compensating controls are in place that could make the vulnerability more difficult to exploit?).

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

The EMC/RSA enterprise GRC council has a focus on cyber security risk that includes the network, and both the vendor provided and company products. Formal processes are in place to assess risk. Other enterprise risks are currently handled in various dispersed forums within EMC.

The internal preparation of our products to meet the demands of customers is tracked within the internal EMC risk framework.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

Broadly speaking ISO 27001, and NIST 800-53 (REV 4) are the baseline security control frameworks in uses at EMC/RSA. However, other specific regulatory needs are address in the context of the environment under the specific regulatory scrutiny, like PCI. EMC/RSA does not simply strive to comply, but rather to manage risk and make smart decisions on a situation-by-situation basis. NIST 800-30 is useful within EMC for Risk Assessments.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

Organizations usually have several regulatory reporting requirements depending on federal, state and local cybersecurity mandates. RSA/Archer provides access to a list of over 90 regulation and frameworks as part of our Policy Management solution. We have domestic and international regulations and frameworks from a wide range of sources and industries: NIST, PCI, SOX, COBIT, COSO, HiTrust, and HIPAA. Archer also provides industry-specific codification and tracking of requirements for healthcare, energy, finance, retail, and transportation. The RSA Archer platform also enables organizations to import specific regulatory content into our solution. In the event RSA Archer doesn't have specific state and local cybersecurity relevant content, organizations can simply import on their own regulatory content and report on it.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

All of the listed infrastructure services are critical to running a business.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Managing cybersecurity risk is a fact of life and has been built into everyday operations. The EMC business teams remain focused on their primary objectives of delivering value to customers. EMC is a

performance driven company that finds the most effective methods of maintaining performance while building a defense-in-depth cybersecurity posture.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

Tools have improved to generate a report with specific requirements from a regulation from a lager set of controls where the regulation may be a subset. The experience on reporting would vary greatly for organizations that can leverage such tools or where the auditors accept a common framework like ISO27001/2 aligned controls from those who manage to each regulation. Improvements are being made to further automate the reporting process for some regulations through reporting formats like XBRL. XBRL has been mandated by a number of regulatory bodies Worldwide as the reporting standard. While it started with financial reporting, it is now moving to the areas of non-financial business information including governance risk and compliance information (controls and risks they mitigate, business processes, tests and related procedures, etc), sustainability reporting, and Carbon disclosure. Many of our customers are operating in multiple jurisdictions and are required to report to a large number of regulators. This is a very costly and challenging task, one that requires working across silos and using standard-based approaches. EMC developed an integrated end-to-end solution to help our customers and to drive the adoption of standards in the financial services and insurance sector. The standards enable support for the secure capture, production, processing, and archiving of XBRL reports for both the regulation and the supervision side of the end-to-end process. XBRL reporting taxonomies will include more and more detailed risk information in the coming years and will integrate additional requirements related to the various types of risks. The XBRL GRC-XML standards taxonomy group is working to align with ISO31000 and other efforts to deliver an open classification of enterprise risks.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Such standards must be practical in their expectations and applicable to global companies. Therefore they should be based on the real world experiences of ICT providers. As security requirements become more visible for the critical infrastructure commercial the adoption of practices and must be scalable.

The role of national/international standards bodies' play in conformance assessments varies and this may depend upon the type of standards published. The IETF for instance, strives to have interoperability between implementations and this works best when the implementation interoperability or conformance testing informs the development of the standard. Reference implementations, conformance testing, or regression testing servers can be very helpful when developing protocols that require interoperability between implementations. As we move further into security automation, ensuring data is represented and exchanged as expected between implementations will be critical. This will be required to assess heterogeneous environments including devices, appliances, and the Internet of Things to the exchange of asset, configuration, threat, vulnerability, incident, and indicator data.

1.2 Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

Industry best practices for secure software are already articulated in the work of industry groups like SAFECode and the Open Group Trusted Technology Forum. ISO has two promising initiatives in this space 27034 and 27036. The upcoming (April) release of the global Open Trusted Technology Provider Standard to Mitigate Maliciously Tainted and Counterfeit Products (O-TTPS) has been developed with joint industry and government consensus. It is planned to be aligned as a reserved ICT COTs part of ISO 27036. EMC/RSA believes that efforts focused on application software are essential to improve security and reduce risk.

Governance, risk and compliance tools are being used by a wide range of organizations within the critical infrastructure to build and publish content for cross sector commentary as well used in the guidelines and standards adoption process. Required capabilities would include workflow, notification, granular access control (permission-based viewing, access and edit rights), reporting capability and an ability to support dedicated views for individual sub-organizations. The ability to consistently assess security through standards will further help to improve the state of security for organizations and service providers.

Control frameworks are widely used today, although the framework may vary depending on the requirements of the organization. The most widely accepted control framework from our experience is the ISO 27000 series because it is an international standard. Country specific frameworks like NIST 800-53 and the Australian control framework are also in use. Tools are often used to map between control frameworks or to map regulatory or policy information into a control framework for simplified management of policies, standards, and controls. In building a secure environment, where risk is prioritized, a baseline set of controls that allows for easy policy comparison between organizations or service providers assists with the governance view of security risk to the organization. RSA has products to support this baseline model. The automation of control validation to the required policy levels is the next logical step in this progression. Various scanning tools exist that use a mix of NIST's SCAP and other scanning techniques. The security control automation work needs further work and EMC/RSA is supportive of the efforts starting in the IETF in Security Automation and Continuous Monitoring (SACM).

The notion of trust assurance levels is covered in FISMA and this level of definition could be useful for international standards to set Service Level requirements or provide a consistent measurement to assert assurance levels between organizations (federated entities, etc.). Although some security automation is in use today, more consistent approaches across infrastructure could be helpful using standards already in place by infrastructure (SACM). Federated identity and access management standards have the ability to assert assurance levels that may be validated through annual audits and through SACM type efforts. PKI certificates can assert the appropriate level of assurance as can SAML in bearer tokens. Mapping between these federation technologies may require further work as not all organizations or systems will operate at the same assurance level or even have a need to operate at the same level.

The ability to assess the posture of systems and applications through SCAP related standards using Network Endpoint Assessment (NEA) or Trusted Network Connect (TNC) helps to maintain the security level of the network and reduce risk. Additionally, the ability to consistently exchange information security incident and indicator information through international standards from the IETF, like IODEF (RFC5070-bis) and RID (RFC6545 andRFC6546) is critical to decision making based on situational awareness. The exchange of information must be meaningful, actionable, and directed. Information sharing must evolve further to connect various types of analysis centers, including those of threat feed providers. Standards in this space can help move us beyond the need for each organization to have highly skilled analysts in order to benefit from information sharing. By including directed and actionable vendor intelligence feeds in the ecosystem, information sharing can scale in that the threat providers will analyze data and push out remediation actions for threats to their customer base as appropriate. This eliminates the requirement for highly skilled analysts at every organization, large or small. The information shared may be limited to rules that get added to host or network based detection and monitoring systems as appropriate. Threat feeds may not include the full picture of an event, as a result of the directed nature of these updates.

For communications to be directed and actionable, only meaningful and useful information should be provided. In the case of incident and indicator sharing, while a portal system for an ISAC may support vast data types to assess threats, the meaningful and actionable data that results from the assessment may be limited to a watchlist of indicators. The watchlist can either be consumed directly into a participants enterprise for actions to be taken or provided to a threat intelligence analysis center for further vetting, where only actionable data is directly sent to their customer base. The latter approach assists with the scalability of information sharing in that fewer highly-skilled resources are needed and threats can be mitigated more quickly across a broad spectrum.

2. Which of these approaches apply across sectors?

These governance, risk, and compliance views of key guidelines for sub-sectors within the critical infrastructure community (power producers, power distributors, natural gas, oil, etc.) must support cross industry collaboration in the Framework development process to ensure all relevant controls are considered. Common frameworks, like the ISO27000 series may provide a baseline for IT systems, but specific industry standards will still be required. The security automation, endpoint assessment, and incident communications described above apply cross-sector, with the need for flexibility and extensibility in each of those standards for sector-specific requirements. In addition to the need for flexibility and continued evolution of a supporting framework, the selected international standards must also be flexible and extensible to accommodate the needs of each sector. "One size does not fit all" applies to the area of extensions that may be unique to each sector, with a common core. The selected standards would ideally be in international standards organizations with transparent processes for developing and updating standards over time.

The communication mechanisms will vary within and across industry sectors or based on use cases. The control frameworks, ability to assert trust assurance levels grounded in security automation capabilities, and cyber threat communication should be consistent, except when extensions are needed to represent industry specific information. The types of communications across sectors may vary and include high level alerting type communications that can be achieved through existing approaches like the Common Alerting Protocol (CAP) from OASIS. NIEM has been exploring the different types of communications needed and may be a starting point to determine what standards may be useful. The ability to apply data sets from different industries could lead to powerful analytic capabilities, such as threat actors in the physical to cyber space. Building off of existing data constructs to support extended

capabilities in spaces like threat actors (OASIS) across sectors may help with the maintenance of those standards over time.

Best practices embodied in the work of SAFECode and the measureable requirements articulated in O-TTPS are able to be levered across sectors and lend themselves to additional tailoring for sector specific actions.

3. Which organizations use these approaches?

RSA Archer has been used in similar capacities to support efforts by the financial sector (BITS) and healthcare sector (HiTrust) as organizations within those communities came together to build sector wide guidelines and standards. In both situations, our capabilities were leveraged to enable cross sector collaboration involving public, private and government organizations who participated in developing sector standards and guidelines. BITS and HiTrust are examples of regulations and control frameworks that can be mapped into security control frameworks described above. These efforts provide consistent methods to compare policies across organizations, which may be very important when establishing federated identity and access management between organizations or even during acquisitions or the selection of service providers. HiTrust is closely aligned with ISO27001/2 and tools like Archer enable automated mapping between regulations and frameworks for consistent comparisons of controls.

4. What, if any, are the limitations of using such approaches?

Education on how to apply the use of control frameworks along with the benefits of aligning to a common set of controls would help to expand their use. There are no short cuts in building defense in depth. Top numbered lists out of context can be misinterpreted as sufficient and they alone do not constitute repeatable practices as part of a program. Efforts like the SANS critical controls to prioritize risks could be better applied within an organization who manages to a control framework. The SANS critical controls evolve as threats evolve over time, therefore using the top 20 SANS controls to prioritize risk in a larger more complete set of controls, managed in an established framework, helps with the management of threat over time. Additionally, while SCAP has brought us a long way towards security automation, security specific management protocols may be a limitation. Security automation is limited platform specific efforts or the areas currently covered by SCAP. Approaches that consider how to leverage the same sets of protocols for IT and security, hopefully through the SACM efforts, will enable better collaboration and management of IT and security within an organization. The IETF effort for security automation may help to overcome these challenges in addition to the ongoing work of SAFECode for secure applications.

The limitation of any national standards is that they don't scale to meet the needs of global customers. Customers in other countries require international standards with transparent processes to consider their requirements and feedback in the design and development of standards. The requirements and practices may vary between nations, and standards may be limited to the areas that require interoperability. This allows for differences to emerge that may be critical for innovation or the specific requirements of an industry or nation.

5. What, if any, modifications could make these approaches more useful?

Active use to inform improvement of the supporting standards in the framework described will be required to support the evolving needs of the community as security automation and information

sharing requirements evolve. Standards supporting the framework should be flexible and extensible, with the ability to update and evolve those standards in a transparent process as needed.

6. How do these approaches take into account sector-specific needs?

The ISO27000 series includes extensions that are industry specific, healthcare, finance, etc. IETF Standards typically consider flexibility and extensibility in their design to allow for standards based or private extensions as appropriate.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

If the overall framework includes flexible and extensible standards based solutions, the referenced standards efforts should have ways to accommodate sector specific needs. Examples where this is true includes the ISO27000 control framework, IETF standards such as the Incident Object Description Exchange Format (IODEF) [RFC5070, in update process RFC5070-bis], and OASIS's Common Alerting Protocol (CAP). Each of these efforts includes methods to extend the standard to accommodate standards based or private extensions specific to the needs of an industry, region, or event type. The extension work should be part of the sector-specific standards development process.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

These agencies and councils could be forums for promoting usage in their sectors, collecting experiences, best practices, etc. The agencies may serve as interfaces between sector participants and standards development of cross-sector frameworks, sector-specific extensions, implementation guidance, etc. Guidance may be appropriate both in standards and in these sector-specific constituencies.

Realizing that some tailoring for a specific sector may be appropriate they should draw from the same acceptable baseline of conformance to best practices and standards.

9. What other outreach efforts would be helpful?

Improved vendor support for international standards in the framework coupled with third party validation for these evolving approaches is critical. Efforts like the NIST Center of Excellence to validate and showcase the capabilities will assist greatly in the outreach. Ensuring that the framework requirements include standards that can evolve over time is critical to innovation in addition to limiting the use of standards to the areas that require interoperability between organizations and products.

Effective outreach should include better educating stakeholders on the myriad of threats that exist to their web application layer, and how behavioral analysis provides a necessary layer of defense. The SANS Critical Controls are a helpful tool for this outreach and education in the prioritization of threats as they evolve.

Additionally, government RFI and contract language should show preference for existing named initiatives that promote best practices and standards.

1.2.1 Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

1. Are these practices widely used throughout critical infrastructure and industry?

In the context of industry, yes, but the degree of maturity in each area can vary widely from place to place, and even across each of these areas in a single company. Our typical experience has noted that cyber security programs will hyper focus in a couple areas and have lower maturity in others, as corporations struggle to fund holistic programs in all areas, a perceived risk based decision is made. Efforts like the SANS critical controls should be used to prioritize risks. Vendors should be supporting efforts to ensure the applications and services they provide are secure through efforts like SAFECode.

The practical best practices such as those recognized by SAFECode and identified in the requirements in the Open Group's upcoming (April) release of the global Open Trusted Technology Provider Standard to Mitigate Maliciously Tainted and Counterfeit Products should pertain to anyone building software and hardware based products.

2. How do these practices relate to existing international standards and practices?

International standards are limited to the control objectives for the listed critical infrastructure components and are not prescriptive in the same way that is true for FISMA related control frameworks with defined assurance levels for controls. The prescriptive requirements from regulations assist organizations in developing their individual policy requirements that may meet or exceed the regulatory requirements for the high-level international standards controls, for instance ISO27001/2. Tools like RSA's Archer are used to bridge this gap so that the varying requirements between organizations can be mapped into common sets of controls, but that the controls may vary between organizations based on requirements. Standards also assist to provide consistent methods to assess the state of controls (SCAP/SACM, NEA, etc.) within an operating environment. International standards also provide consistent data formats and protocols to enable to exchange of information between organizations

(MILE, CAP, etc.). And at the base, applications must be secure before we even start to think about the ongoing or continuous assessment of an environment (SAFECode, OpenGroup work, ISO27036).

SAFECode is a global industry group of practitioners that share best practices and guidance. The Open Group O-TTPS is likely to be submitted through the PAAS process for COTS ICT applicability to ISO 27036 for supplier relationships.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

Improved standards and capabilities for understanding situational awareness through automated assessment and enforcement of policies for the environment is critical for secure operations. This includes the ability to understand threats to organizations assets, active exploits against vulnerabilities, and the ability to prioritize risk as a result of having a common operating picture.

The SAFECode guidance and best practices and the set of requirements in the Open Group O-TTPS outline a baseline of what is most important to promote the secure operation of critical infrastructure.

NIST's work in crypto standards and federation technology and practices will become increasingly more important in a hyper connected world. As we move to cloud based environments with federated access between cloud environments to facilitate big data analytics, the use of federation via technologies like PKI and SAML will only increase. While encryption and key management are absolutely critical, we believe continuous monitoring of encrypted data streams is absolutely critical. We have seen even the most sophisticated encryption methods defeated through the most low technology means, e.g. social engineering. We believe monitoring should be non intrusive - it should not affect the legitimate user's experience nor impede the delivery of data and resources.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

5. Which of these practices pose the most significant implementation challenge?

Security automation presents some of the more difficult challenges, where approaches need to be generalized to include devices and many areas of infrastructure (Internet of Things) for capabilities in each sector. The interconnected federation models (PKI, SAML) need to support trust assurance assertions (PKI OIDs and SAML bearer tokens) with the varying use of technologies also presents a challenge where these technologies intersect.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

Where interoperability is required, EMC/RSA strictly follows the applicable standards. For instance, DMTF's Common Information Model (CIM), IETF standards for protocols (TCP, HTTP, TLS, SNMP, PKI, RID), OMG's standards for reporting (GRC-XML), XBRL, numerous NIST standards, and ISO standards such as the 27000 series for control frameworks, policy, and risk management.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Yes, business stakeholders participate in every step of the governance process for IT standards with the EMC Corporate Office of the CTO, central cyber security organization, and the product security organization. The Corporate Office of the CTO leads the external standards efforts in collaboration with

all key stakeholders, while the central cyber security organization and product security organization support the internal standards efforts. The business allocates funds toward remediation management activities when needed, and balances the risks of cyber security against other business objectives.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Yes, EMC/RSA has formal escalation processes in place for risks that suddenly increase in severity.

RSA tools also support the detection and analytic capabilities for risks in the environment. While this work includes a mix of internal process and areas that require flexibility for innovation, points that interface with other products may be considered in the framework for standards. The following description provides insight into tools that may be used to compliment the cyber security framework, but are areas where standards may not apply to allow for innovation, standards should be limited to interfaces where interoperability is required.

Security analytics systems should have the sophistication to combine disparate data to detect indicators of advanced attacks. For example, security analytics systems should search for behavior patterns and risk factors, not just static rules and known signatures. Security analytics systems should also consider the relative value of enterprise assets at risk, flagging events associated with high-value assets. By applying a risk-based approach leveraging big data, security analytics platforms can eliminate "known good" activities and improve the signal-to-noise ratio, slashing the amount of information that security analysts must review in their hunt for new threats to the enterprise. Deeper, automated analytics present items of interest to security analysts, reporting "this happens a lot" or "this rarely happens." This provides a formal approach to escalation where the alert is validated, thus making the response more efficient and effective. By doing this, security analytics systems can perform triage for security analysts, highlighting events that require a closer look. While automated, intelligent analytics are an important component of new security analytics platforms, they don't take the place of human judgment; instead they spotlight areas where human judgment, with its unique organizational and domain expertise, should be applied. In essence, security analytics systems help SOCs scale their threat detection capabilities in ways that weren't possible before, helping analysts make sense of incidents in time to make a difference in the outcome of an advanced attack.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

Information security and compliance professionals rarely agree on how security tools such as full network capture should be used to prevent or detect internal and external attacks. Compliance professionals are more likely to believe that surveillance of employees can be effectively accomplished without diminishing employees' privacy rights and that securing the workplace from illegal or unauthorized activities is not as important as ensuring employees' privacy rights. In contrast, security professionals tend to believe in the requirement and legitimacy of surveillance to protect their organizations.

There exists a continual balance between threat monitoring and personal privacy. Effective cyber threat monitoring does not necessarily require an overarching approach to data capture. Technology needs to provide the ability to encode sensitive data values (e.g. SSN) that pass between the user and a web server. These encoded values are still useful for threat modeling, but do not give cyber operators complete visibility into the user's communication with the web server.

The challenge for organizations concerned with addressing the risks of both internal and external threats is to ensure that the fragile balance between privacy and security is properly and consistently

applied across the enterprise. As noted above, achieving agreement requires practitioners dedicated to information security and compliance professionals to collaborate closely to close gaps and avoid silos, especially when it concerns employee's privacy rights.

10. What are the international implications of this Framework on your global business or in policymaking in other countries? Show citation box

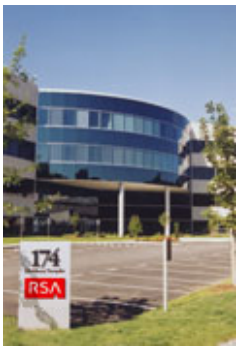
The use of international standards is critical as EMC/RSA operates on a global scale, both as an organization and as a technology provider. Standards are selected for implementation to meet the broad needs of our user base, favoring international standards whenever possible. Standards should only be used when there is a need for interoperability between implementations, leaving room for innovation in areas like data analytics and providing advanced intelligence. International standards that maintain transparent development and update procedures make it possible for global organizations and customers to improve the selected standards as the needs and requirements of each change.

11. How should any risks to privacy and civil liberties be managed?

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

2 Corporate Overview

RSA at a glance
■ **Employees**: 2,800+ worldwide as part of EMC's 47,800+ global employees.
■ **Customers**: 35,000+ globally, using RSA solutions to protect 455+ million consumers, and deploying 1+ billion BSAFE applications and 20+ million SecurID tokens



RSA, the Security Division of EMC, is the premier provider of security, risk, and compliance management solutions for business acceleration. RSA helps the world's leading organizations solve their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption and key management, DLP, Security Analytics and Network Security Monitoring and Analysis, and fraud protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform, and the data that is generated.

2.1 An enviable heritage

For over two decades, businesses have trusted RSA to secure e-business. Our lineage can be traced back to 1977 when Ronald L. Rivest, Adi Shamir, and Leonard Adleman invented the RSA algorithm. Today, RSA, The Security Division of EMC, is the expert in information-centric security:

RSA / EMC Corporation Milestones			
1977	Invention of RSA algorithm	**2007**	EMC acquires Verid, Inc. (KBA solutions) and adds to RSA EMC acquires Tablus Inc. (DLP solutions) and adds to RSA
1979	EMC Corporation founded		
1982	RSA Data Security founded		
1984	Security Dynamics Technologies, Inc. founded SecurID solutions launched	**2010**	EMC acquires Archer Technologies (eGRC solutions) and adds to RSA
1986	EMC listed on NASDAQ	**2011**	EMC acquires NetWitness Corporation (network security analysis solutions) and adds to RSA
1988	EMC listed on NYSE		
1991	RSA Laboratories established	**2012**	EMC acquires Silicium Security (endpoint monitoring tool for unknown and advanced malware detection) and adds to RSA RSA launches Advanced Cyber Defense Services RSA Laboratories develops and launches RSA Distributed Credential Protection EMC acquires Silver Tail Systems (web fraud detection and security software) and adds to RSA RSA opens new Anti-Fraud Command Center in Collaboration with Purdue University
1992	EMC achieves ISO 9001 certification		
1994	EMC enters Fortune 500		
1996	Acquisition of RSA Data Security by Security Dynamics Technologies, Inc.		
1999	Company fully integrates and becomes RSA Security Inc.		
2005	Acquisition of Cyota Inc. (online security and anti-fraud solutions)		
2006	Acquisition of PassMark Security Inc. (software-based authentication) Acquisition of RSA by EMC Corporation. Becomes RSA, the Security Division of EMC	**2013**	RSA launches RSA Security Analytics

2.2 Technology and Business Solutions

RSA's industry leading solutions are designed to work together to create a systematic approach to managing security, risk, and compliance: eliminating the hundreds of security and compliance silos that

exist in most organizations today. Our technology solutions for physical, virtual and cloud computing environments include:

- **Advanced Cyber Defense (ACD) Services**: The RSA ACD Practice is designed to address the need for agile mitigation of APT attacks. Using a multi-tier threat based approach; ACD focuses on the protection of critical business assets by applying proven operational design and tactics to address front line cyber breach preparedness, response, remediation, and prevention.
- **Authentication**: RSA offers a wide range of strong two-factor authentication solutions to help organizations assure user identities and meet compliance requirements. Choices include one-time passwords, risk-based authentication, knowledge-based authentication, and digital certificates. RSA authentication solutions are available in a variety of form factors including hardware authenticators, software authenticators delivered across a range of mobile devices and platforms, out-of-band phone and SMS options, and site-to-user authentication. Products include:
    - RSA Adaptive Authentication, RSA Digital Certificate Manager, RSA Identity Verification, and RSA SecurID
- **Data Loss Prevention (DLP)**: The RSA DLP solution identifies and enforces policies to prevent the loss or misuse of sensitive data: whether at rest in a data center, in motion over the network, or in use on a laptop or desktop.
- **Data Protection**: RSA encryption and tokenization solutions secure sensitive data stored in file systems on servers and endpoints and at the point of capture. RSA key management solutions offer a common infrastructure to simplify the provisioning, distribution and management of encryption keys. Product include:
    - RSA BSAFE, RSA Distributed Credential Protection, and RSA Data Protection Manager
- **Fraud Prevention**: RSA fraud prevention solutions reduce the risk of fraud and identity theft by assuring user identities, monitoring for high-risk activities, and mitigating the damage caused by external threats such as phishing, pharming, Trojans, and other cyber threats. Products include:
    - RSA Adaptive Authentication eCommerce, RSA CyberCrime Intelligence Service, RSA eFraudNetwork, RSA Fraud Action, and RSA Transaction Monitoring
- **Governance, Risk, and Compliance (GRC)**: The RSA Archer GRC solutions enable organizations to manage the lifecycle of corporate policies and objectives across a number of domains; analyze and respond to enterprise risk and demonstrate compliance. Through a series of easy-to-read dashboards and reports, RSA GRC solutions provide organizations with a real-time view into their state of compliance and risk level.
- **Identity and Access Management**: RSA solutions manage access, federate identities, and enforce organizational policies across multiple web resources, portals, and applications. These solutions make it easy to manage a large number of users while enforcing a centralized security policy, ensuring compliance and preventing unauthorized access to corporate systems and sensitive information. Products include:
    - RSA Access Manager, RSA Adaptive Directory, RSA Adaptive Federation, and RSA Federated Identity Manager
- **Security Analytics and Network Security Monitoring and Analysis:** The RSA Security Analytics platform provides a complete and actionable understanding of network sessions as well as logs and events activity happening on enterprise networks. The RSA Security Analytics solutions are flexible and scalable to solve a wide range of the most challenging information

security problems including: compliance, forensic analysis, insider threats, zero-day exploits and targeted malware, advanced persistent threats, fraud, espionage, data leakage, and continuous monitoring of critical security controls.

- **Professional Services**: RSA Professional Services helps organizations successfully implement high-value security solutions based on RSA industry-leading technology. Leveraging the expertise of its Professional Services organization, RSA brings together the technology, services, and expertise necessary to develop and implement a comprehensive information security strategy.
- **Security Consulting**: The RSA Security Practice of EMC Consulting approaches security from a business context that prioritizes security investments. Services from the RSA Security Practice of EMC Consulting specialize in both security policy and compliance areas such as PCI DSS and HIPAA/HITECH and span across areas such as data classification, information risk management, GRC and policy management, fraud mitigation, identity assurance, virtualization and security operations.

2.3 Commitment to Interoperability

The Secured by RSA technology partner program is one of the largest and most proven alliance programs of its type. Through over 1,000 strategic partnerships with industry-leading organizations, RSA is able to integrate its solutions into many diverse environments. The Secured by RSA program focuses on interoperability certification activities as well as joint support strategies for our mutual customers. Certification brings added assurance that the solutions we provide are interoperable with industry-leading security products. The program reflects RSA commitment to providing standards-based interoperability and mutual vendor support to customers using our products and solutions.

2.4 RSA Thought Leadership

RSA is committed to investing in the ongoing development and improvement of our existing security solutions and bringing new products, ideas, and knowledge to the market. RSA has two world-renowned centers - RSA Laboratories and the RSA Anti-Fraud Command Center – dedicated to advancing security research and intelligence and staying up-to-date on the latest global threats.

- **RSA Laboratories**: RSA Laboratories is the research center of RSA and the security research group within the EMC Innovation Network. Established in 1991, RSA Laboratories is world renowned for applied research program and academic connections that provide state-of-the-art expertise in cryptography and data security for the benefit of RSA, EMC, and our customers. Recent projects have included cloud security, data protection, tamper-resistant hardware schemes, efficient fully homomorphic encryption (FHE) computations, and privacy-preserving computations.
- **RSA Online Fraud Resource Center**: RSA's 24x7 Anti-Fraud Command Center (AFCC) leads the global fight against "external threats" - such as phishing, crimeware/Trojans, and pharming attacks - by working with thousands of ISPs, registrars, and other hosting entities worldwide to mitigate and shut down attacks. The AFCC is staffed with more than 150 analysts, and has shut down over 580,000 online attacks.
- **Standards Development**: RSA also plays an active leadership role in standards development initiatives – such as Liberty Alliance, OASIS, IETF, and WS-Security – to ensure the technical

superiority and interoperability of our solutions. Our current products support a multitude of standards, including PKCS, RADIUS, and SAML.

2.5 Financial Strength and Corporate Stability

As the Security Division of EMC, we are part of a global Fortune 500 organization, and benefit from the financial strength, stability, and depth of resources of EMC:

- Revenue exceeding $21.7 billion
- A 5-year annual revenue growth rate of 10.42%
- Market capitalization of approximately $51.5 billion
- Research & Development exceeding $2.5 billion
- Dun & Bradstreet rating of "5A2" since 2004
- Standard & Poor's credit rating of "A-/STABLE" since 2008

Please refer to the following link for comprehensive details of EMC's financials http://www.emc.com/ir, and the following summary table:

In millions of USD	2012	2011	2010	2009	2008
Total Revenue	**21,713.90**	**20,007.59**	**17,015.13**	**14,025.91**	**14,876.16**
Cost of Revenue	8,075.54	7,838.65	6,984.15	6,281.01	6,653.79
Gross Profit	**13,638.36**	**12,168.94**	**10,030.98**	**7,744.90**	**8,222.37**
Research & Development	2,559.61	2,149.79	1,888.02	1,627.51	1,721.33
Total Operating Expense	**17,750.03**	**16,565.15**	**14,331.84**	**12,661.64**	**13,307.23**
Operating Income	3,963.87	3,442.44	2,683.29	1,414.28	1,568.94
Net Income Before Taxes	**3,803.62**	**3,249.27**	**2,607.98**	**1,374.58**	**1,600.23**
Cash & Short Term Investments	6,167.12	6,318.02	5,375.31	6,695.34	6,806.98
Total Current assets	**12,208.61**	**11,702.22**	**9,783.32**	**10,538.30**	**10,665.03**
Property / Plant / Equipment, Total - Net	3,144.55	2,833.15	2,528.43	2,224.35	2,223.01
Total Assets	**38,068.69**	**34,469.27**	**30,833.28**	**26,812.00**	**23,874.58**
Total Current Liabilities	**10,304.00**	**10,376.21**	**9,378.01**	**5,148.17**	**5,218.44**
Total Debt	1,710.15	3,424.30	3,450.00	3,100.29	2,991.94
Total Liabilities	**15,711.54**	**15,157.65**	**13,429.24**	**11,262.12**	**10,546.13**
Total Equity	**22,537.14**	**19,311.61**	**17,404.04**	**15,549.88**	**13,328.44**

2.6 EMC / RSA Company Vitals

Details	EMC Corporation	RSA, the Security Division of EMC
Primary Address	176 South Street Hopkinton, MA 01748 USA	174 Middlesex Turnpike Bedford, MA 01730 USA
Contact Numbers	Phone: 508−435−1000 / 877−362−6973 Fax: 508−497−6912	Phone: 781−515−5000 / 877−772−4900 Fax: 781−515−5010

Details	EMC Corporation	RSA, the Security Division of EMC
Senior Management Team	Joseph M. Tucci – Chairman and CEO William J. Teuber, Jr. – Vice Chairman David I. Goulden – President and COO	Arthur W. Coviello, Jr. - Executive Chairman Thomas P. Heiser - President
# of Employees	47,800	2,800
Web Site	www.emc.com	www.emc.com/rsa
Doing Business As:	EMC^2	RSA Security LLC
Year of Founding	1979	1982
State of Incorporation	MA	DE
Federal Tax ID (US)	04-2680009	27-1492791
DUNS:	097447148	121615538
CAGE Code:	0DVT5	5Z940
EMC Investor Relations:	http://www.emc.com/corporate/investor-relations/index.htm	
EMC Corporate Governance:	http://www.emc.com/corporate/investor-relations/governance/corporate-governance.htm	
EMC Sustainability:	http://www.emc.com/corporate/sustainability/index.htm	
EMC Newsroom	http://www.emc.com/about/news/index.htm	
RSA Standard Agreements	http://www.emc.com/support/rsa-standard-form-agreements.htm	
EMC Certificate of Insurance	https://online.marsh.com/marshconnectpublic/marsh2/public/moi?PID=AppMoiFAQ-Terms&CLIENT=900094051	
Reps and Certs	https://www.sam.gov/portal/public/SAM/ (search records using Company Name, DUNS, or CAGE code)	