HITRUST
Health Information Trust Alliance

Framework for Reducing Cyber Risks to Critical Infrastructure

Response from the Health Information Trust Alliance (HITRUST)

Perspective

Many of the questions within the NIST RFI are geared towards gathering information from industry regarding their processes and controls. For example, "where do organizations locate their cyber security risk management program/office?" Responses from HITRUST to these questions are provided in consideration of the requirements of the CSF related to the question, and where possible, observations and feedback from the industry.

Current Risk Management Practices

Q1. What do organizations see as the greatest challenges in improving cyber security practices across critical infrastructure?

The greatest challenge for many organizations is balancing the breadth and depth of what should be done to mitigate cyber security risks with significant limitations on skills, man-power, and budgets. There are many standards, regulations, and frameworks available that provide prescriptive controls addressing a comprehensive information security program, such as NIST, ISO, PCI and the HITRUST CSF. However, identifying the current state of the environment, prioritizing remediation actions, and implementing controls can take a great deal of time and money. Even small organizations with a limited scope of assets and information to protect lack the necessary capabilities and resources to address all aspects of security in an acceptable timeframe. In healthcare, this is highlighted in a 2009 Life Sciences and Health Care Study by Deloitte, which cited "budget constraints and/or lack of resources" as the predominant barrier to implementing IT security for Providers (59.18% of respondents noted this as an issue).

While budgets and resource constraints cannot be directly addressed via a framework, HITRUST and other federal programs such as Meaningful Use have seen success in gaining adoption and making progress for IT security through a focused, phased approach. The objective is to break down the full set of controls and requirements that should be implemented by organizations, and prioritize them over a multi-year period. This gives organizations a more manageable set of areas to focus on each year, address the critical issues first, and spread out the costs and time of implementing controls.

This is the approach HITRUST has taken with its Certification Program in the healthcare industry. HITRUST recognized that the industry needed a common baseline of security that all organizations could achieve and work from, that the baseline needed to be a subset of the full set of controls from the CSF that prioritized the highest risks (most likely to cause a breach or lead to the highest impact breaches) in the industry, and that the bar needed to be ratcheted up over time to achieve continuous improvement across the board.

Q2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

The greatest challenges HITRUST has experienced in developing and maintaining its Common Security Framework (CSF) for the healthcare industry have been providing the prescriptiveness and clarity organizations seek while making the controls scalable to organizations and systems of a variety of sizes, risk profiles, and capabilities.

HITRUST works with and provides guidance to organizations with less than 10 employees up to $100B national corporations. The capabilities of each varies dramatically as does the risk profile of each (i.e., large companies have more patient records and more points of exposure than smaller companies). HITRUST provides a set of requirements that is scalable tor various size organizations by providing up to three levels of controls, a concept leveraged from NIST's risk management framework. HITRUST expanded upon this concept by providing a specific set of risk factors that trigger increasing levels of control. For example, a small organization with less than 100 employees may only be required to assign an individual with shared responsibility for security (i.e., security is one of perhaps many roles they hold). An organization with between 101 and 1,000 employees may be required to have a dedicated security, privacy, and compliance officer. Finally, an organization with over 1,000 employees may be required to have a dedicated set of officers, with team leaders or points of contact spread throughout each business unit, who are governed by a formal information security steering committee. In each example, the intent of the control is the same (i.e., managing the information security program) but the implementation of the control is scaled to organizations of various sizes considering their risk factors and nominal capability for this control, which in this example is measured by employee count.

This scalability while maintaining a significant level of prescriptiveness has allowed the HITRUST CSF to become the most widely adopted security controls framework in healthcare, as it is broadly applicable to all organizations in the industry but can be tailored to each organization's unique risks and characteristics.

Given the difficulties encountered in the adoption of a common framework in healthcare—a rather diverse sector in and of itself—HITRUST believes similar difficulties will be found in a multi-sector framework. However, we firmly believe the lessons learned by HITRUST—as well as the lessons learned by NIST in the development of a common framework for the defense, intelligence and federal civilian agencies—can be used to develop and gain successful adoption of a common critical infrastructure framework. Approval of such a framework by federal regulators, including various safe harbor provisions for the implementation of the cross-industry framework, will also significantly enhance its acceptance and improve the rate of adoption.

Q3. Describe your organization's policies and procedures governing risk generally and cyber security risk specifically. How does senior management communicate and oversee these policies and procedures?

The HITRUST CSF requires four controls related to information security risk management: Risk Management Program Development, Performing Risk Assessments, Risk Mitigation, and Risk Evaluation. Risk Management Program Development requires organizations to develop a comprehensive risk management strategy related to security, including the creation of policies, performance of risk assessments, mitigation of risks, and reassessment and update to the policies. Performing Risk Assessments requires organizations to perform periodic risk assessments using a framework of controls as the baseline and considering the likelihood and impact of threats and vulnerabilities. Risk Mitigation requires organizations to address risk by avoidance, reduction, transference, or acceptance, and document the criteria by which the means to address risk can be determined. Finally, Risk Evaluation requires organizations to periodically, at least annually, re-evaluate their risk management program and make updates for improvements or changes to the environment.

The HITRUST CSF requires management to coordinate the implementation and enforcement of security and risk management by:

- identifying by name or position non-professional or professional security contacts in each major organizational area or business unit;
- creating an internal security information sharing mechanism, such as an e-mail group, periodic conference call or standing meeting; and
- providing supplemental security education and training activities for the organization's distributed security contacts;

These requirements are derived from COBIT, the CMSRs, ISO, NIST, HIPAA, PCI and multiple state regulations.

With respect to communication, HITRUST recognized the increasing risks posed by cyber attacks and growing concerns about the state of cybersecurity within the healthcare industry and established the HITRUST Cyber Threat Intelligence and Incident Coordination Center (C3) approximately 18 months ago. The HITRUST C3 relies upon a community defense approach to enable the industry's preparedness and response to cyber threats and attacks. It facilitates early identification, coordinated response and incident tracking, as well as knowledge sharing and enhanced preparedness for healthcare organizations challenged by cyber attacks.

The center is focused on cybersecurity threats and events targeted at healthcare organizations in areas, including, but not limited to, networks, mobile devices, workstations, servers, applications and medical devices. The center is also working with the U.S. Department of Health and Human Services to timely share various incident information and for participation in the Critical Infrastructure Information Sharing and Collaboration Program (CISCP). This sharing of information is crucial for organizations' preparedness, protection and crisis management. HITRUST will also lead the center's participants in evaluating appropriate tools and related security mechanisms to support the center's efforts.

Also available through HITRUST C3 is the HITRUST Cyber Threat Analysis Service (CTAS), which aims to help healthcare organizations prioritize their cybersecurity efforts and raise security awareness by informing them of general and sector-specific threats impacting the industry.

Q4. Where do organizations locate their cyber security risk management program/office?

HITRUST requires that organizations appoint a senior-level manager/executive for information security risk management. For larger organizations, this is supplemented by requiring a Security Advisory Board, Security Steering Committee, or other governing body, and by identifying points of contact throughout the organization who can work with the manager and governing bodies to implement controls, effect policy changes, and communicate with the workforce.

However, HITRUST has found that many organizations, especially smaller ones, place the information security official one or two levels below the Chief Information Officer (CIO) or equivalent. This generally results in less visibility to senior leadership and a focus on technical information security issues rather than a broad-based information protection program. Increased emphasis by federal regulators on a suitable level and full integration into enterprise governance processes could help improve the viability of a healthcare organization's information protection program.

Q5. How do organizations define and assess risk generally and cyber security risk specifically?

HITRUST takes the generally accepted approach of looking at risk as a function of the likelihood and impact of a threat exploiting a vulnerability but takes a somewhat different, control-oriented approach focused on either risk of a breach or risk of non-compliance. We found that the theoretical exercise of identifying all possible threat and vulnerability pairs and identifying the likelihood and impact of each pair to be far too labor intensive for organizations in healthcare considering the possible benefits. Given the comprehensive nature of the HITRUST CSF, instead we identified the cyber security risk of not implementing a control considering both likelihood (i.e., the characteristics of the organization or system that would increase the possibility of experiencing a breach or being out of compliance with a regulatory requirement) and non-contextual impact (i.e., the loss or disclosure of PHI). This is demonstrated through the organizational, system and regulatory risk factors contained in the CSF. The number of controls required for a certification assessment has increased from 45 of 135 in 2009 to 63 of 135 in 2013. Like the OCR Audit Protocol, an organization obtains specific efficiencies and cost savings associated with a targeted assessment of high risk controls. However, HITRUST expects an organization to fully address all the controls applicable to their specific risk factors, and will incorporate a random sample of the remaining controls in certification assessments beginning with the 2014 CSF release.

HITRUST has also recently made changes to the previous compliance-oriented assessment approach to incorporate quasi-quantitative estimates of likelihood and impact of a specific control failure. A “likelihood estimator” for the likelihood of a control failure is computed based on an assessment of control maturity adopted from NIST Interagency Report (NISTIR) 7358, Program Review for Information Security Management Assistance (PRISMA). Likelihood estimates of relative impact are derived from an analysis performed by the Department of Defense (DoD) on the controls contained in DoD Instruction 8500.2, Information Assurance (IA) Implementation. These estimates provide a non-contextual assessment of relative risk, which allows an organization to focus their attention on a residual risk analysis of a smaller subset of controls with identified deficiencies.

Healthcare organizations can use the HITRUST C3 and supporting services to help them focus on specific cybersecurity threats on a real and near real-time basis. In addition, HITRUST has identified a specific subset of CSF controls that are most relevant to cybersecurity and is in the process of vetting these controls through a working group of healthcare industry representatives. Organizations will be able to then evaluate their level of cybersecurity preparedness through a focused assessment similar to the CSF certification assessment. This will allow organizations to benchmark their state of readiness against other, similar organizations and the industry as a whole. The assessment can also provide a baseline by which organizations can evaluate control remediation and other cybersecurity improvement efforts.

Q6. To what extent is cyber security risk incorporated into organizations' overarching enterprise risk management?

The HITRUST CSF requires organizations to develop a [cyber security] risk management program. As part of the implementation of this requirement, organizations must define the objectives of the program and processes, management's level of acceptable risk, and the connection between risk management and the strategic planning processes. These requirements and their associated activities should be nested within the organization's enterprise-wide risk management program. For example, the risk appetite of the organization should be defined for the enterprise, which can then be leveraged in the development of the organization's cyber security risk management program. The same is true for the objectives of the program and the planning processes (i.e., they should reflect the objectives of the enterprise wide risk management program, which in turn should reflect the objectives of the business).

However, many healthcare organizations do not fully integrate information security risk management in their overarching enterprise risk management programs, which has historically resulted in little if any senior management governance of information security risk issues. (In fact, some organizations do not have an enterprise-level risk management program at all.) Fortunately HITRUST is starting to see improvements in governance and enterprise-level integration, in large part due to increased incentives and penalties in recent federal and state legislation (e.g., HITECH and Texas H.B. 300).

Q7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

HITRUST's approach to helping organizations understand, measure and manage risk at all levels is rooted in federal guidance, considers fundamental requirements and is tailored for the unique risks in healthcare. The HITRUST CSF Assurance Program and supporting tools were developed and have been continually enhanced since the frameworks inception, e.g., the incorporation of the PRISMA information security maturity model. For each requirement that organizations must evaluate as part of an assessment, the organization must identify their current state across each level of the maturity model and generally obtain a level 3 (implemented) for each risk area or domain of the assessment. HITRUST provides guidance for levels 4 (measured) and 5 (managed); however these levels are not required for certification. The assessment domains also incorporate the minimum necessary requirements to address the required and addressable implementation specifications of the HIPAA Security Rule and HITECH Breach Notification Rule, both of which are fundamental compliance requirements that all healthcare organizations and their business associates must meet. HITRUST supplements this with an analysis of high risk areas in healthcare resulting in the greatest loss of PHI and thus ensures an organization addresses a core set compliance and risk elements in healthcare.

The HITRUST assessment process is built upon the MyCSF tool, which leverages GRC tool capabilities to facilitate data gathering, reporting, remediation management, and benchmarking. This more sophisticated level of tool support has become necessary to support the increasingly complex environments of healthcare entities, which consist of multiple disparate facilities and systems that may be controlled in different ways and subsequently by different people. Without this type of tool, individuals are generally left managing their assessment and remediation efforts with spreadsheets and other document, which can be time-consuming, resource-intensive, and provide little support for decision makers in the way of aggregate or summary reporting and analysis.

Q8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cyber security?

The HITRUST CSF is not a new standard or regulation; it's a harmonized framework that incorporates and cross-references the existing federal, state, third party and business requirements and standards that organizations must address. This means the burden of compliance with the CSF is no more than what organizations must already meet (but often do not given the inherent complexity of managing multiple requirements and programs). The CSF simply provides an industry-developed and accepted approach to understand the overlap and relationship of each requirement and address security in a prioritized and practical way.

Currently HITRUST incorporates the security requirements of the following sources:

- ISO/IEC27001:2005
- ISO/IEC27002:2005
- ISO/IEC27799:2008
- COBIT 5
- HIPAA
- NIST SP 800-53 Revision 4
- NIST SP 800-66
- PCIDSS version 2.0
- 16CFR Part 681
- FTC Red Flags Rule
- HITECH Act
- 21CFR Part 11
- JCAHOIM
- 201 CMR 17.00 (State of Mass.)
- NRS 603A (State of Nev.)
- CSA Cloud Controls Matrix v1
- CMSARS
- TXHB 300
- CAQHCORE

Organizations may select one or more of the above sources that apply to their environment and a single set of requirements that addresses all of the security requirements of each source. Where there is overlap between two or more sources, the requirements are unified, allowing organizations to take an "assess once, report many" approach to security and compliance.

Q9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Public health concerns would indicate that telecommunications are critical to healthcare providers and other public health organizations. Delivery of healthcare is also highly dependent on power and, to a lesser extent, water infrastructure support.

Q10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cyber security risk?

Performance goals vary widely among the various types of healthcare organizations and are generally tied to specific business and clinical goals. Healthcare providers will likely rely on existing and future meaningful use measures and other criteria promulgated by industry organizations such as the American Hospital Association and the Joint Commission. However, HITRUST has seen very little integration of information security goals and measures with business and clinical goals as part of their overall governance processes. Information security is generally only reviewed when an issue may adversely impact one or more business or clinical goals. HITRUST sees this as an opportunity for future guidance and support.

Q11. 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?

While HITRUST is not required to report to aregulatory body, anecdotal evidence would suggest that many healthcare organizations have treated these requirements as separate programs and have not historically leveraged a harmonized set of requirements to support an "assess once, report many" approach. This is a principal focus of HITRUST, the CSF and the CSF Assurance Program.

Q12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cyber security conformity assessment?

HITRUST was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. Although compliance with HIPAA was already required, the Security Rule's lack of prescriptiveness led to varying interpretations and implementations in controls and non-standard reporting to external parties, such as customers or business partners. In turn, organizations could not gain the confidence necessary to share information with each other without spending the time and resources to conduct proprietary, independent reviews of security.

An important element of HITRUST is that the requirements were not new, they were existing requirements molded into a common framework that applies and scales to all organizations in healthcare. Organizations in healthcare already had a multitude of security requirements and standards. By offering a framework that makes compliance with those requirements and standards easier and offering a way to assess and report that compliance in fewer steps with fewer resource expenditures, HITRUST has been able to grow the CSF and CSF Assurance Program into the most widely adopted security framework and certification program in healthcare. Without this level of standardization brought by HITRUST, organizations would not have a clear, common set of expectations for security, which in turn leads to increased costs and risk.

By (1) leveraging and harmonizing multiple international, national, industry and other best practice standards, guidance and frameworks and (2) providing a mechanism for managed scoping and tailoring of requirements to the specific needs of an organization, the HITRUST CSF clearly demonstrates a common security framework is not only possible, it is quite practical. A similar approach should be taken to develop a cybersecurity framework for critical infrastructure across multiple industry sectors. Formal recognition by federal, state and industry regulators—supported by appropriate incentives such as safe harbor for those that implement the framework in good faith—will also help improve acceptance across multiple sectors and result in a higher probability of successful adoption.

Use of Frameworks, Standards, Guidelines and Best Practices

Q1. What additional approaches already exist?

HITRUST provides the CSF freely to covered entities and their business associates in the healthcare industry. The CSF is not a new standard; the CSF is a framework that incorporates and cross-references the existing standards and regulations applicable to the healthcare industry. This means the burden of adopting the CSF is no more than what organizations are already obligated to do. The CSF provides benefits in its prescriptiveness, comprehensiveness and scalability, meaning organizations can bypass the process of documenting and cross-referencing their requirements and then tailor those requirements to their unique environment—the CSF already represents this and was done through an open, industry-wide and industry-accepted approach.

The CSF Assurance Program provides the tools, methodology and requirements to become Certified with respect to security in the healthcare industry. This streamlined approach to assessing the core controls related to the fundamental compliance requirements in healthcare (e.g., HIPAA) and highest risks allows organizations to reduce the burden of security in the exchange of information. Without the CSF Assurance Program, organizations connecting with each other had no means of evaluating and gaining assurance that their information will be safe in the hands of their partner, customer or service provider. This resulted in organizations conducting and undergoing numerous, repeated, proprietary audits, which wasted time and money assessing risk rather than actively managing risk. With the advent of the CSF Assurance Program, healthcare organizations can now conduct a single assessment against a common set of criteria and report the results of that assessment to multiple third parties. HITRUST provides an additional layer of validation by evaluating and issuing all reports conducted under the CSF Assurance Program. Because the approach and requirements are standardized, third parties can rely on the results with confidence.

Q2. Which of these approaches apply across sectors?

HITRUST and the CSF Assurance Program are currently focused on the healthcare industry and the security of protected health information (PHI). The CSF, which forms the basis of the CSF Assurance Program, can be used as the basis of control for sensitive information other than ePHI. The CSF is built upon ISO 27001 and 27002, the international standards for information security risk management. HITRUST supplemented the controls from ISO with other comprehensive and industry agnostic standards and guidance including NIST SP 800-53, NIST SP 800-66 and COBIT. In addition, the CSF incorporates other industry vertical requirements such as the Payment Card Industry (PCI) Digital Security Standard (DSS) and the Cloud Security Alliance (CSA) Cloud Controls Matrix. Because the CSF is scalable and flexible, organizations using the framework can choose and implement only those controls which relate to the standards and regulations that apply to their environment. This was purposefully integrated into the CSF since HITRUST and our constituents understood that many organization in and outside of healthcare store a variety of sensitive information beyond PHI and would need a solution that their third party service providers could also adopt.

Q3. Which organizations use these approaches?

HITRUST is governed by an Executive Council comprised of Highmark, UnitedHealth Group, IMS Health, Express Scripts, WellPoint, Humana, Kaiser Permanente, and McKesson. HITRUST CSF Assessors, the professional services firms uniquely qualified to provide CSF related services, includes AT&T Consulting, BluePrint Healthcare IT, Booz Allen Hamilton, Coalfire Systems, Deloitte & Touche, Epstein Becker & Green, Ernst & Young, Fortrex Technologies, Lattimore Black Morgan & Cain, Marlabs, PricewaterhouseCoopers, Protiviti, SecureInfo, Solutionary, UHY Advisors, and Verizon Business. And today the HITRUST Central community is populated with over 5200 members with CSF adoption of over 60% of hospitals and 70% of health plans in the U.S. HITRUST does not publicize a list of organizations using the CSF or Certified under the CSF Assurance Program; however a few organizations have themselves publicized their Certification such as HCMS Group, Availity, WellTok, and FireHost.

Note the CSF Assurance Program and Certification could be expanded to apply more broadly across a variety of industries that provide critical infrastructure such as financial services, energy, water, and telecommunications. Adoption of a new Certification for security in these other industries could be slow, as it was with healthcare, and it could take between 3 and 5 years before there is a general awareness and acceptance of the Certification in these other industries unless there is strong advocacy by federal regulators.

Q4. What, if any, are the limitations of using such approaches?

Certification under the CSF Assurance Program does not include all controls and requirements from the CSF. This was done deliberately to account for the state of information security in the industry and provide specific efficiencies for the assessment and mitigation of risk. The healthcare industry has struggled with the adoption of security due to budget and resource constraints, the complex nature of their environment, and the slow adoption of IT in general. While security is now progressing much more swiftly due to new regulations such as the HITECH Act, updates to the HIPAA Security Rule, and programs such as Meaningful Use, it was and remains necessary to set an attainable bar for organizations with respect to security that will be raised over time. HITRUST justifies the requirements of the CSF Assurance Program for Certification by aligning with the core compliance requirements of HIPAA and HITECH supplemented by controls which mitigate the highest risks of experiencing a breach in healthcare. The result is approximately 1/2 of the controls of the CSF being required for Certification. The CSF Assurance Program also supports business relationships where PHI is being shared.

A specific limitation of this approach is the limited assurances that a compliance-based gap analysis of a subset of controls provide. However, HITRUST is in the process of updating the HITRUST CSF Assurance Program methodology to account for these limitations (see Q5 below).

Q5. What, if any, modifications could make these approaches more useful?

Although risk is considered in the selection of controls required for certification, the assessment and reporting methodology does not currently provide the more granular risk analysis advocated by NIST. This has been left to the healthcare organization in much the same way as the NIST HIPAA Security Rule Toolkit. To address these limitations, HITRUST has incorporated quasi-quantitative estimates of likelihood and impact of a specific control failure into the methodology. A "likelihood estimator" for the likelihood of a control failure is computed based on an assessment of control maturity adopted from NIST Interagency Report (NISTIR) 7358, Program Review for Information Security Management Assistance (PRISMA). Likelihood estimates of relative impact are derived from an analysis performed by the Department of Defense (DoD) on the controls contained in DoD Instruction 8500.2, Information Assurance (IA) Implementation. These estimates provide a non-contextual assessment of relative risk, which allows an organization to focus their attention on a residual risk analysis of a smaller subset of controls with identified deficiencies to provide contextual estimates of risk and support (1) identification of specific risk treatments and (2) prioritization of specific remediation activities/projects. And beginning with the 2014 CSF release, the CSF Assurance program will also require organizations to assess a random sample of controls that are not required for 2014 CSF Certification to help ensure organizations are addressing all the controls applicable to their specific risk factors.

Q6. How do these approaches take into account sector-specific needs?

HITRUST is focused on serving the needs of the healthcare industry with respect to the privacy, security and compliance challenges the industry faces. The HITRUST CSF considers a variety of compliance requirements in healthcare including HIPAA, HITECH, CMS ARS, ISO 27799, JCAHO, CAQH CORE, and many State requirements. The CSF was built to scale to maintain applicability to organizations of varying size and complexity in the healthcare industry. It also provides segment-specific risk factors which are used to tailor the controls of the CSF and achieve the scalability previously mentioned.

The CSF Assurance Program is designed to make information sharing between healthcare entities (covered entities and business associates) less burdensome. The program establishes a common set of requirements applicable to healthcare considering compliance (e.g., HIPAA, HITECH) and the highest risks resulting in the greatest loss of PHI. The requirements currently represent a subset of the full requirements of the CSF to make Certification more attainable to healthcare organizations which have traditionally struggled with security. Over time, these requirements are increased, raising the bar and moving the industry forward with security.

Q7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

HITRUST found that when developing the CSF, the framework needed to be flexible to account for the different challenges and requirements faced by healthcare organizations. For example, healthcare providers have different requirements (e.g., Joint Commission) and different considerations (e.g., patient safety) than other segments such as health plans. HITRUST overcame this challenge by designing the framework in such a way that allows organizations to select their risk and compliance characteristics and obtain a set of controls that applies to them based on those characteristics. In some instances, it was necessary for HITRUST to further distinguish certain requirements within controls through segment-specific sections. These sections identified additional requirements only applicable to a certain segment that would be included in addition to the core set of controls. Using healthcare providers once again as an example, additional control requirements must be considered or certain requirements modified in situations where emergency care is being provided and security could significantly impact a physician's ability to provide that care. For instance, with authentication, the CSF provides a segment-specific requirement for providers allowing tokens, smartcards or biometrics in place of passwords (not in addition to passwords) which can allow a physician to more quickly authenticate to provide the necessary care (e.g., tapping a smartcard to authenticate as opposed to typing in a password).

HITRUST believes a similar approach would be necessary on a broader scale, where a core framework can be established that is flexible and can incorporate additional sector-specific requirements where needed. The approach would be very similar to the federal government's own transformation initiative, which integrates the risk management frameworks of federal civilian agencies and the defense and intelligence communities.

Q8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

The requirements and risks in the healthcare industry are constantly changing—new standards and regulations are released or updates to existing requirements are made. HITRUST has kept pace with these changes in healthcare to ensure the CSF and CSF Assurance Program remains relevant and maintain the trust of the healthcare industry. HITRUST also provides a level of quality control by ensuring assessing organizations are qualified to conduct healthcare information protection assessments and provide assurances around the validity of certification assessments. Further, because of the large community of participants using the CSF, HITRUST has been able to actively seek and receive feedback on key risk areas, either through the CSF or CSF Assurance Program itself or other sources such as training and cyber threat monitoring. Other sector-specific agencies like HITRUST outside of healthcare could provide a similar value and reduce the burden and cost of a single agency maintaining awareness of all sector changes, developing relationships with the organizations operating within the sector, and gaining assurances around assessor organizations and the assessments they conduct.

Q9. What other outreach efforts would be helpful?

HITRUST believes there is little competitive advantage to addressing issues of security independently. There exist broad challenges that all industries and organizations face, which are noted in the Specific Industry Practices section of the RFI. In addition to an overarching framework supported by industry-specific standards, HITRUST recommends establishing communities across all industries to foster communication and sharing between security professionals and leaders. As noted in the prior question, sector-specific agencies or coordinating councils such as HITRUST could be charged with overseeing these industry-specific communities. The communities could consist of periodic leadership events with keynote presentations and more tactical learning tracks that address specific topics, mailing lists or online messaging systems, industry-specific training for personnel, and threat monitoring and coordination. Participation in such communities should be open to all industry stakeholders; however restrictions should be in place to limit services and technology vendor participation to maintain focus and ensure the continued integrity of the community.

Specific Industry Practices

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.

Q1. Are these practices widely used throughout critical infrastructure and industry?

Yes. Within healthcare and the CSF, these practices are principally addressed as follows:

Practice	HITRUST CSF Reference
Separation of business from operational systems	• 01.w Sensitive System Isolation • 09.d Separation of Development, Test and Operational Environments • 09.w Interconnected Business Information Systems • 10.h Control of Operational Software
Use of encryption and key management	• 06.d Data Protection and Privacy of Covered Information • 10.f Policy on the Use of Cryptographic Controls • 10.g Key Management
Identification and authorization of users accessing systems	• 01.b User Registration • 01.j User Authentication for External Connections • 01.q User Identification and Authentication
Asset identification and management	• 07.a Inventory of Assets • 07.b Ownership of Assets • 07.d Classification Guidelines
Monitoring and incident detection tools and capabilities	• 09.n Security of Network Services • 09.aa Audit Logging • 09.ab Monitoring System Use • 09.ae Fault Logging
Incident handling policies and	• 11.a Reporting Information Security Events

Practice	HITRUST CSF Reference
procedures	• 11.b Reporting Security Weaknesses • 11.c Responsibilities and Procedures • 11.d Learning from Information Security Incidents • 11.e Collection of Evidence
Mission/system resiliency practices	• 09.l Backup • 10.m Control of Technical Vulnerabilities • 12.a Including Information Security in the Business Continuity Management Process • 12.b Business Continuity and Risk Assessment • 12.c Developing and Implementing Continuity Plans Including Information Security • 12.d Business Continuity Planning Framework • 12.e Testing, Maintaining and Reassessing Business Continuity Plans
Security engineering practices	• 10.a Security Requirements Analysis and Specification
Privacy and civil liberties protection	• 06.d Data Protection and Privacy of Covered Information

Q2. How do these practices relate to existing international standards and practices?

Based on the cross-references between the CSF and other standards and regulations, these practices relate as follows:

Practice	HITRUST CSF Reference
Separation of business from operational systems	• CMSRs 2010v1 SC-4 • CMSRs 2010v1.0 CA-3 (HIGH) • CMSRs 2010v1.0 CM-2 (HIGH) • COBIT 4.1 DS5.10 • COBIT 4.1 DS5.11 • COBIT 5 DSS05.02 • CSA SA-06 • HIPAA §164.308(b)(1) • HIPAA §164.308(b)(4) • HIPAA §164.314(a)(2)(ii) • ISO 27002 11.6.2 • ISO 27799 7.8.5.2 • ISO 27799-2008 7.7.1.4

Practice	HITRUST CSF Reference
	• ISO 27799-2008 7.7.8.4 • ISO/IEC 27002-2005 10.1.4 • ISO/IEC 27002-2005 10.8.5 • NIST 800-53 R4 SC-4 • NIST SP800-53 R4 CA-3 • NIST SP800-53 R4 CM-2 • NRS 603A.215.1 • PCI DSS v2 1.2 • PCI DSS v2 2.2.1 • PCI DSS v2 6.3.1 • PCI DSS v2 6.3.2 • PCI DSS v2 6.4.1 • PCI DSS v2 6.4.3 • PCI DSS v2 6.4.4
Use of encryption and key management	• CMSRs 2010v1.0 IA-7 (HIGH) • CMSRs 2010v1.0 PL-5 (HIGH) • CMSRs 2010v1.0 SC-12 (HIGH) • CMSRs 2010v1.0 SC-13 (HIGH) • CMSRs 2010v1.0 SC-13(1) (HIGH) • CMSRs 2010v1.0 SI-12 (HIGH) • COBIT 4.1 DS5.8 • COBIT 5 DSS05.03 • CSA IS-18 • CSA IS-19 • Guidance to render PHI unusable, unreadable, or indecipherable (a) • Guidance to render PHI unusable, unreadable, or indecipherable (a)(i) • Guidance to render PHI unusable, unreadable, or indecipherable (a)(ii) • HIPAA §164.312(a)(2)(iv) • HIPAA §164.312(e)(2)(ii) • ISO 27799-2008 7.12.2.2 • ISO 27799-2008 7.9.2.1 • ISO 27799-2008 7.9.3.1 • ISO/IEC 27002-2005 12.3.1 • ISO/IEC 27002-2005 15.1.4 • JCAHO IM.02.01.03, EP 2 • JCAHO IM.02.01.03, EP 6 • NIST SP800-53 R4 IA-7 • NIST SP800-53 R4 SC-12 • NIST SP800-53 R4 SC-13

Practice	HITRUST CSF Reference
	• NIST SP800-53 R4 SI-12 • NRS 603A.210.1 • NRS 603A.215.1 • NRS 603A.215.2.a • PCI DSS v2 3.4 • PCI DSS v2 3.4.1 • PCI DSS v2 3.5.2 • PCI DSS v2 3.6.6 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • TX Gen. Laws § 181.004(a)
Identification and authorization of users accessing systems	• (State of Mass.) 201 CMR 17.04(2)(a) • (State of Mass.) 201 CMR 17.04(2)(b) • (State of Mass.) 201 CMR 17.04(1)(a) • (State of Mass.) 201 CMR 17.04(1)(d) • (State of Mass.) 201 CMR 17.04(2)(b) • 16 CFR Part §681 Appendix A III(b) • CMSRs 2010v1.0 AC-17 (HIGH) • CMSRs 2010v1.0 AC-17(1) (HIGH) • CMSRs 2010v1.0 AC-17(3) (HIGH) • CMSRs 2010v1.0 AC-17(4) (HIGH) • CMSRs 2010v1.0 AC-17(5) (HIGH) • CMSRs 2010v1.0 AC-17(7) (HIGH) • CMSRs 2010v1.0 AC-18 (HIGH) • CMSRs 2010v1.0 AC-18(1) (HIGH) • CMSRs 2010v1.0 AC-2 (HIGH) • CMSRs 2010v1.0 AC-2(3) (HIGH) • CMSRs 2010v1.0 IA-1 (HIGH) • CMSRs 2010v1.0 IA-2 (HIGH) • CMSRs 2010v1.0 IA-2(8) (HIGH) • CMSRs 2010v1.0 IA-4 (HIGH) • CMSRs 2010v1.0 IA-5 (HIGH) • CMSRs 2010v1.0 IA-5(2) (HIGH) • CMSRs 2010v1.0 IA-5(3) (HIGH) • CMSRs 2010v1.0 IA-8 (HIGH) • COBIT 4.1 DS5.3 • COBIT 4.1 DS5.4 • COBIT 5 DSS05.03 • COBIT 5 DSS05.04 • CSA IS-08

Practice	HITRUST CSF Reference
	• CSA SA-07 • HIPAA §164.308(a)(3)(i) • HIPAA §164.308(a)(3)(ii)(A) • HIPAA §164.308(a)(3)(ii)(B) • HIPAA §164.308(a)(4)(i) • HIPAA §164.308(a)(4)(ii)(B) • HIPAA §164.308(a)(4)(ii)(C) • HIPAA §164.308(a)(5)(ii)(C) • HIPAA §164.308(a)(5)(ii)(D) • HIPAA §164.310(c) • HIPAA §164.312(a)(2)(i) • HIPAA §164.312(a)(2)(ii) • HIPAA §164.312(d) • ISO 27799-2008 7.8.2.1 • ISO 27799-2008 7.8.4 • ISO 27799-2008 7.8.5.1 • ISO/IEC 27002-2005 11.2.1 • ISO/IEC 27002-2005 11.4.2 • ISO/IEC 27002-2005 11.5.2 • JCAHO IM.02.01.03, EP 5 • NIST SP800-53 R4 AC-17 • NIST SP800-53 R4 AC-17(1) • NIST SP800-53 R4 AC-17(3) • NIST SP800-53 R4 AC-17(4) • NIST SP800-53 R4 AC-18 • NIST SP800-53 R4 AC-18(1) • NIST SP800-53 R4 AC-2 • NIST SP800-53 R4 AC-2 (3) • NIST SP800-53 R4 IA-1 • NIST SP800-53 R4 IA-2 • NIST SP800-53 R4 IA-2(3) • NIST SP800-53 R4 IA-2(8) • NIST SP800-53 R4 IA-4 • NIST SP800-53 R4 IA-5 • NIST SP800-53 R4 IA-5(2) • NIST SP800-53 R4 IA-5(3) • NIST SP800-53 R4 IA-8 • NRS 603A.215.1 • PCI DSS v2 12.3.9 • PCI DSS v2 12.5.4 • PCI DSS v2 2.3 • PCI DSS v2 3.2

Practice	HITRUST CSF Reference
	• PCI DSS v2 8.1 • PCI DSS v2 8.2 • PCI DSS v2 8.3 • PCI DSS v2 8.5.1 • PCI DSS v2 8.5.4 • PCI DSS v2 8.5.5 • PCI DSS v2 8.5.6 • PCI DSS v2 8.5.7 • PCI DSS v2 8.5.8 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 1 CORE 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.1 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • TX Gen. Laws § 181.004(a)
Asset identification and management	• CMSRs 2010v1.0 CM-8 (HIGH) • CMSRs 2010v1.0 CM-8(1) (HIGH) • CMSRs 2010v1.0 CM-8(2) (HIGH) • CMSRs 2010v1.0 CM-8(4) (HIGH) • CMSRs 2010v1.0 CM-8(5) (HIGH) • CMSRs 2010v1.0 RA-2 (HIGH) • CSA DG-01 • CSA DG-02 • CSA FS-08 • HIPAA §164.308(a)(1)(ii)(A) • HIPAA §164.308(a)(1)(ii)(B) • HIPAA §164.308(a)(1)(ii)(E) • HIPAA §164.310(d)(1) • HIPAA §164.310(d)(2)(iii) • ISO 27799-2008 7.4.1 • ISO 27799-2008 7.4.2.1 • ISO/IEC 27002-2005 7.1.1 • ISO/IEC 27002-2005 7.1.2 • ISO/IEC 27002-2005 7.2.1 • JCAHO IM.02.01.03, EP 5 • NIST SP800-53 R4 CM-8 • NIST SP800-53 R4 CM-8(1) • NIST SP800-53 R4 CM-8(5) • NIST SP800-53 R4 PM-5 • NIST SP800-53 R4 RA-2 • NRS 603A.215.1

Practice	HITRUST CSF Reference
	• PCI DSS v2 12.3.3 • PCI DSS v2 12.3.4 • PCI DSS v2 9.9.1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • TX Gen. Laws § 181.004(a)
Monitoring and incident detection tools and capabilities	• (State of Mass.) 201 CMR 17.04(4) • (State of Mass.) 201 CMR 17.03(2)(h) • 16 CFR Part §681 Appendix A III(b) • 16 CFR Part §681.2 (e)(4) • CMSRs 2010v1.0 AU-6 (HIGH) • CMSRs 2010v1.0 AU-6(1) (HIGH) • CMSRs 2010v1.0 AU-7 (1) (HIGH) • CMSRs 2010v1.0 AU-7 (HIGH) • CMSRs 2010v1.0 CA-3 (HIGH) • CMSRs 2010v1.0 SA-9 (HIGH) • CMSRs 2010v1.0 SC-8 (HIGH) • CMSRs 2010v1.0 SC-8(1) (HIGH) • CMSRs 2010v1.0 SC-9 (HIGH) • CMSRs 2010v1.0 SC-9(1) (HIGH) • CMSRs 2010v1.0 SI-4 (HIGH) • CMSRs 2010v1.0 SI-4(1) (HIGH) • CMSRs 2010v1.0 SI-4(2) (HIGH) • CMSRs 2010v1.0 SI-4(3) (HIGH) • CMSRs 2010v1.0 SI-4(4) (HIGH) • CMSRs 2010v1.0 SI-4(5) (HIGH) • CMSRs 2010v1.0 SI-4(6) (HIGH) • CSA IS-31 • CSA SA-14 • HIPAA §164.213(c)(2) • HIPAA §164.308(a)(1)(ii)(D) • HIPAA §164.308(a)(3)(ii)(A) • HIPAA §164.308(a)(4)(i) • HIPAA §164.308(a)(4)(ii)(B) • HIPAA §164.308(a)(5)(ii)(B) • HIPAA §164.308(a)(5)(ii)(C) • HIPAA §164.308(b)(1) • HIPAA §164.308(b)(4) • HIPAA §164.312(b) • HIPAA §164.312(c)(1)

Practice	HITRUST CSF Reference
	• HIPAA §164.312(e)(1) • HIPAA §164.312(e)(2)(i) • HIPAA §164.312(e)(2)(ii) • HIPAA §164.314(a)(1) • HIPAA §164.314(a)(2)(ii) • ISO 27799-2008 7.7.10.3 • ISO 27799-2008 7.7.6.2 • ISO/IEC 27002-2005 10.10.2 • ISO/IEC 27002-2005 10.6.2 • ISO/IEC 27002-2005 12.5.4 • NIST SP800-53 R4 AU-6 • NIST SP800-53 R4 AU-6 (1) • NIST SP800-53 R4 AU-6 (9) • NIST SP800-53 R4 AU-7 • NIST SP800-53 R4 AU-7 (1) • NIST SP800-53 R4 CA-3 • NIST SP800-53 R4 SA-9 • NIST SP800-53 R4 SC-8 • NIST SP800-53 R4 SC-8(1) • NIST SP800-53 R4 SC-9 • NIST SP800-53 R4 SC-9(1) • NIST SP800-53 R4 SI-4 • NIST SP800-53 R4 SI-4(2) • NIST SP800-53 R4 SI-4(4) • NIST SP800-53 R4 SI-4(5) • NIST SP800-53 R4 SI-4(6) • NRS 603A.215.1 • PCI DSS v2 10.6 • PCI DSS v2 11.5 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • TX Gen. Laws § 181.004(a)
Incident handling policies and procedures	• (State of Texas) HB 300 521.053(b) • (State of Texas) HB 300 521.053(b-1) • (State of Mass.) 201 CMR 17.03(2)(j) • 16 CFR Part §681 Appendix A II(c) • 16 CFR Part §681 Appendix A IV(a) • 16 CFR Part §681 Appendix A IV(b) • 16 CFR Part §681 Appendix A IV(c) • 16 CFR Part §681 Appendix A IV(d)

Practice	HITRUST CSF Reference
	• 16 CFR Part §681 Appendix A IV(e) • 16 CFR Part §681 Appendix A IV(f) • 16 CFR Part §681 Appendix A IV(g) • 16 CFR Part §681 Appendix A IV(h) • 16 CFR Part §681 Appendix A IV(i) • CMSRs 2010v1.0 IR-1 (HIGH) • CMSRs 2010v1.0 IR-3 (HIGH) • CMSRs 2010v1.0 IR-3(1) (HIGH) • CMSRs 2010v1.0 IR-4 (HIGH) • CMSRs 2010v1.0 IR-4(1) (HIGH) • CMSRs 2010v1.0 IR-5 (HIGH) • CMSRs 2010v1.0 IR-5(1) (HIGH) • CMSRs 2010v1.0 IR-6 (HIGH) • CMSRs 2010v1.0 IR-6(1) (HIGH) • CMSRs 2010v1.0 IR-7 (HIGH) • CMSRs 2010v1.0 IR-7(1) (HIGH) • CMSRs 2010v1.0 IR-8 (HIGH) • CMSRs 2010v1.0 PL-4 (HIGH) • CMSRs 2010v1.0 SI-2 (HIGH) • CMSRs 2010v1.0 SI-4 (HIGH) • CMSRs 2010v1.0 SI-5 (HIGH) • COBIT 4.1 DS5.6 • COBIT 5 DSS02.01 • CSA IS-22 • CSA IS-23 • CSA IS-24 • CSA IS-25 • HIPAA §164.308(a)(1)(ii)(D) • HIPAA §164.308(a)(5)(ii)(A) • HIPAA §164.308(a)(5)(ii)(B) • HIPAA §164.308(a)(6)(i) • HIPAA §164.308(a)(6)(ii) • HIPAA §164.314(a)(2)(i) • HITECH Act, Subpart D 164.404(a)(1) • HITECH Act, Subpart D 164.404(a)(2) • HITECH Act, Subpart D 164.404(b) • HITECH Act, Subpart D 164.404(c)(1) • HITECH Act, Subpart D 164.404(c)(2) • HITECH Act, Subpart D 164.404(d)(1) • HITECH Act, Subpart D 164.404(d)(2) • HITECH Act, Subpart D 164.404(d)(3) • HITECH Act, Subpart D 164.406(a)

Practice	HITRUST CSF Reference
	• HITECH Act, Subpart D 164.406(b) • HITECH Act, Subpart D 164.406(c) • HITECH Act, Subpart D 164.408(a) • HITECH Act, Subpart D 164.408(b) • HITECH Act, Subpart D 164.408(c) • HITECH Act, Subpart D 164.410(a)(1) • HITECH Act, Subpart D 164.410(a)(2) • HITECH Act, Subpart D 164.410(b) • HITECH Act, Subpart D 164.410(c)(1) • HITECH Act, Subpart D 164.410(c)(2) • HITECH Act, Subpart D 164.412 • HITECH Act, Subpart D 164.414(b) • ISO 27799-2008 7.10.1 • ISO 27799-2008 7.10.2.1 • ISO 27799-2008 7.10.2.2 • ISO 27799-2008 7.10.2.3 • ISO/IEC 27002-2005 13.1.1 • ISO/IEC 27002-2005 13.1.2 • ISO/IEC 27002-2005 13.2.1 • ISO/IEC 27002-2005 13.2.2 • ISO/IEC 27002-2005 13.2.3 • NIST SP800-53 R4 IR-1 • NIST SP800-53 R4 IR-3 • NIST SP800-53 R4 IR-3(2) • NIST SP800-53 R4 IR-4 • NIST SP800-53 R4 IR-4(1) • NIST SP800-53 R4 IR-5 • NIST SP800-53 R4 IR-6 • NIST SP800-53 R4 IR-6(1) • NIST SP800-53 R4 IR-7 • NIST SP800-53 R4 IR-7(1) • NIST SP800-53 R4 IR-8 • NIST SP800-53 R4 PL-4 • NIST SP800-53 R4 PM-12 • NIST SP800-53 R4 SI-2 • NIST SP800-53 R4 SI-4 • NIST SP800-53 R4 SI-5 • NRS 603A.215.1 • NRS 603A.220.1 • NRS 603A.220.2 • NRS 603A.220.3 • NRS 603A.220.4.a

Practice	HITRUST CSF Reference
	• NRS 603A.220.4.b • NRS 603A.220.4.c.1 • NRS 603A.220.4.c.2 • NRS 603A.220.4.c.3 • NRS 603A.220.6 • PCI DSS v2 12.5.2 • PCI DSS v2 12.5.3 • PCI DSS v2 12.9 • PCI DSS v2 12.9.1 • PCI DSS v2 12.9.2 • PCI DSS v2 12.9.3 • PCI DSS v2 12.9.4 • PCI DSS v2 12.9.5 • PCI DSS v2 12.9.6 • PCI DSS v2 A.1.4 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • TX Gen. Laws § 181.004(a)
Mission/system resiliency practices	• (State of Mass.) 201 CMR 17.04(6) • CMSRs 2010v1.0 CM-7 (HIGH) • CMSRs 2010v1.0 CP-1 (HIGH) • CMSRs 2010 v1.0 CP-2 (HIGH) • CMSRs 2010 v1.0 CP-2 (1) (HIGH) • CMSRs 2010 v1.0 CP-2 (2) (HIGH) • CMSRs 2010 v1.0 CP-2 (3) (HIGH) • CMSRs 2010 v1.0 CP-4 (4) (HIGH) • CMSRs 2010 v1.0 CP-6 (HIGH) • CMSRs 2010 v1.0 CP-6 (1) (HIGH) • CMSRs 2010 v1.0 CP-6 (2) (HIGH) • CMSRs 2010 v1.0 CP-6 (3) (HIGH) • CMSRs 2010 v1.0 CP-7 (HIGH) • CMSRs 2010 v1.0 CP-7 (1) (HIGH) • CMSRs 2010 v1.0 CP-7 (2) (HIGH) • CMSRs 2010 v1.0 CP-7 (3) (HIGH) • CMSRs 2010 v1.0 CP-7 (4) (HIGH) • CMSRs 2010 v1.0 CP-7 (5) (HIGH) • CMSRs 2010v1.0 CP-8 (HIGH) • CMSRs 2010v1.0 CP-8 (1) (HIGH) • CMSRs 2010v1.0 CP-8 (2) (HIGH) • CMSRs 2010v1.0 CP-8 (3) (HIGH)

Practice	HITRUST CSF Reference
	• CMSRs 2010v1.0 CP-8 (4) (HIGH) • CMSRs 2010 v1.0 CP-9 (HIGH) • CMSRs 2010 v1.0 CP-9 (2) (HIGH) • CMSRs 2010v1.0 CP-10 (HIGH) • CMSRs 2010v1.0 CP-10 (2) (HIGH) • CMSRs 2010v1.0 CP-10 (3) (HIGH) • CMSRs 2010v1.0 CP-10 (4) (HIGH) • CSA DG-04 • CSA RS-01 • CSA RS-02 • HIPAA §164.308(a)(7)(i) • HIPAA §164.308(a)(7)(ii)(A) • HIPAA §164.308(a)(7)(ii)(B) • HIPAA §164.308(a)(7)(ii)(C) • HIPAA §164.308(a)(7)(ii)(D) • HIPAA §164.308(a)(7)(ii)(E) • HIPAA §164.310(a)(2)(i) • HIPAA §164.310(a)(2)(ii) • HIPAA §164.310(d)(2)(iv) • HIPAA §164.310(d)(2)(v) • HIPAA §164.312(c)(1) • HIPAA §164.312(c)(2)(ii) • ISO 27799-2008 7.9.5 • ISO/IEC 27002-2005 10.5.1 • ISO/IEC 27002-2005 12.6.1 • ISO/IEC 27002-2005 14.1.3 • ISO 27799-2008 7.7.5 • ISO 27799-2008 7.11 • JCAHO IM.01.01.03 EP 2 • JCAHO IM.01.01.03 EP 3 • JCAHO IM.01.01.03 EP 4 • NIST SP800-53 R4 CM-7 • NIST SP800-53 R4 CP-1 • NIST SP800-53 R4 CP-2 • NIST SP800-53 R4 CP-2 (1) • NIST SP800-53 R4 CP-2 (2) • NIST SP800-53 R4 CP-2 (3) • NIST SP800-53 R4 CP-2 (8) • NIST SP800-53 R4 CP-6 • NIST SP800-53 R4 CP-6 (1) • NIST SP800-53 R4 CP-6 (3) • NIST SP800-53 R4 CP-7

Practice	HITRUST CSF Reference
	• NIST SP800-53 R4 CP-7 (1) • NIST SP800-53 R4 CP-7 (2) • NIST SP800-53 R4 CP-7 (3) • NIST SP800-53 R4 CP-8 • NIST SP800-53 R4 CP-8 (1) • NIST SP800-53 R4 CP-8 (2) • NIST SP800-53 R4 CP-9 • NIST SP800-53 R4 CP-10 • NIST SP800-53 R4 CP-10 (2) • NIST SP800-53 R4 CP-10 (3) • NIST SP800-53 R4 RA-5 • NIST SP800-53 R4 RA-5(1) • NIST SP800-53 R4 PM-8 • NIST SP800-53 R4 SI-2 • NRS 603A.215.1 • PCI DSS v2 11.2 • PCI DSS v2 11.2.1 • PCI DSS v2 11.2.2 • PCI DSS v2 11.2.3 • PCI DSS v2 12.9.1 • PCI DSS v2 2.2 • PCI DSS v2 6.2 • PCI DSS v2 6.4.5 • PCI DSS v2 6.4.5.1 • PCI DSS v2 6.4.5.2 • PCI DSS v2 6.4.5.3 • PCI DSS v2 6.4.5.4 • PCI DSS v2 9.5 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • TX Gen. Laws § 181.004(a).
Security engineering practices	• CMSRs 2010v1.0 SA-1 (HIGH) • CMSRs 2010v1.0 SA-3 (HIGH • CMSRs 2010v1.0 SA-4 (1) (HIGH) • CMSRs 2010v1.0 SA-4 (2) (HIGH) • CMSRs 2010v1.0 SA-4 (3) (HIGH) • CSA IS-04 • ISO/IEC 27002-2005 12.1.1 • HIPAA §164.314(a)(2)(i) • NIST SP800-53 R4 SA-1

Practice	HITRUST CSF Reference
	• NIST SP800-53 R4 SA-3 • NIST SP800-53 R4 SA-4 (1) • NIST SP800-53 R4 SA-4 (4) • NIST SP800-53 R4 PM-7 • NRS 603A.214.1. • PCI-DSS v2 6.3
Privacy and civil liberties protection	• CMSRs 2010v1.0 PL-5 (HIGH) • CMSRs 2010v1.0 SI-12 (HIGH) • CSA IS-18 • Guidance to render PHI unusable, unreadable, or indecipherable (a)(i) • Guidance to render PHI unusable, unreadable, or indecipherable (a)(ii) • ISO 27799-2008 7.12.2.2 • ISO 27799-2008 7.9.2.1 • ISO/IEC 27002-2005 15.1.4 • JCAHO IM.02.01.03, EP 2 • NIST SP800-53 R4 SI-12 • NRS 603A.210.1 • NRS 603A.215.1 • PCI DSS v2 3.4 • PCI DSS v2 3.4.1

Q3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

HITRUST develops certification criteria as part of its CSF Assurance Program. The certification criteria represent the subset of controls from the CSF that organizations must comply with in order to be HITRUST Certified. These requirements are focused on addressing fundamental compliance requirements in healthcare (HIPAA, HITECH) as well as those areas resulting in the greatest number of breaches of PHI. HITRUST and its participants see the following high level domains as the most critical areas of security for healthcare:

HITRUST Certification Domain	Description
Information Protection Program	Includes the information security management system (ISMS)
Endpoint Protection	Includes requirements common to laptops, workstations, storage (e.g., NAS) and servers
Portable Media Security	Includes mobile storage (e.g., USB drives, CD-ROMs, DVD-ROMs, backup tapes)

HITRUST Certification Domain	Description
Mobile Device Security	Includes requirements specific to laptops, smart phones and tablets
Wireless Security	Includes all aspects of corporate and guest wireless networks but does not include protections for devices connected to other networks
Configuration Management	Includes all aspects of configuration management (e.g., configuration item identification, configuration status accounting, change control and configuration audit)
Vulnerability Management	Includes the formal vulnerability management program (e.g., vulnerability scanning and patching)
Network Protection	Includes all aspects of perimeter and internal network security
Transmission Protection	Includes Web and network connections (e.g., VPN, email, chat)
Password Management	Addresses specific issues around the use of traditional passwords
Access Control	Includes all aspects of access control other than the use of traditional passwords (e.g., provisioning)
Audit Logging & Monitoring	Includes all aspects of audit logging and monitoring
Education, Training and Awareness	Includes the education and training of specialized security personnel as well as the standard user; includes an overall, ongoing (continuous) awareness program/campaign
Third Party Assurance	Addresses all aspects of managing risk associated with third parties (e.g., vendors, business associates)
Incident Management	Includes incident monitoring and detection activities, incident response and breach reporting
Business Continuity & Disaster Recovery	Includes all aspects of contingency, business continuity and disaster recovery (e.g., planning, implementation, exercise/testing)
Risk Management	Includes risk assessment, analysis, and other risk management-related activities
Physical & Environmental Security	Includes the physical and environmental security requirements for data centers and other facilities containing sensitive information, as well as disposal and destruction of sensitive information
Data Protection & Privacy	Addresses the organization's compliance and privacy program and related controls

A cross reference matrix between the detailed controls that support these areas and the practices of interest to NIST are listed below:

Practice	HITRUST CSF Reference Required for Certification	Certification Domain
Separation of business from operational systems	01.w Sensitive System Isolation	Network Protection
	09.d Separation of Development, Test and Operational Environments	Not Required for HITRUST Certification for 2013
	09.w Interconnected Business Information Systems	Not Required for HITRUST Certification for 2013
	10.h Control of Operational Software	Configuration Management
Use of encryption and key management	06.d Data Protection and Privacy of Covered Information	Data Protection & Privacy
	10.f Policy on the Use of Cryptographic Controls	Transmission Protection
	10.g Key Management	Transmission Protection
Identification and authorization of users accessing systems	01.b User Registration	Access Control
	01.j User Authentication for External Connections	Access Control
	01.q User Identification and Authentication	Access Control
Asset identification and management	07.a Inventory of Assets	Vulnerability Management
	07.b Ownership of Assets	Not Required for HITRUST Certification for 2013
	07.d Classification Guidelines	Not Required for HITRUST Certification for 2013
Monitoring and incident detection tools and capabilities	09.n Security of Network Services	Not Required for HITRUST Certification for 2013
	09.ab Monitoring System Use	Audit Logging & Monitoring
Incident handling policies and procedures	11.a Reporting Information Security Events	Incident Management
	11.b Reporting Security Weaknesses	Not Required for HITRUST Certification for 2013
	11.c Responsibilities and Procedures	Incident Management
	11.d Learning from Information Security Incidents	Not Required for HITRUST Certification for 2013
	11.e Collection of Evidence	Not Required for HITRUST Certification for 2013
Mission/system resiliency practices	10.m Control of Technical Vulnerabilities	Vulnerability Management
Security engineering	None noted	N/A

Practice	HITRUST CSF Reference Required for Certification	Certification Domain
practices		
Privacy and civil liberties protection	06.d Data Protection and Privacy of Covered Information	Data Protection & Privacy

The CSF already incorporates the controls that would address cybersecurity threats and notes that any assessment should be incorporated into an organization's broader risk and regulatory compliance and assessment strategy. But given the heightened sensitivity and increasing threat, organizations may want to perform an assessment that focuses specifically on cybersecurity. As such, HITRUST has identified specific CSF controls that are highly related to cybersecurity—or more specifically to the prevention of cyber intrusions by external human threat actors and their identification and response when preventative safeguards fail. The table below separates all 135 CSF controls into three categories based on their assessed relevance to cybersecurity threats: Most Relevant, Relevant, and Least Relevant.

CSF Controls – Most Relevant	CSF Controls –Relevant (Requires Further Analysis)	CSF Controls – Least Relevant
01.a* - Access Control Policy	0.a*- Information Security Management Program	01.g – Unattended User Equipment
01.b* - User Registration	01.c – Privilege Management	01.h – Clear Desk and Clear Screen Policy
01.d* - User Password Management	01.e – Review of User Access Rights	01.k – Equipment Identification in Networks
01.f* - Review of User Access Rights	01.l – Remote Diagnostic and Configuration Port Protection	01.p – Secure Log-on Procedures
01.i* - Policy on the User of Network Services	01.s – Use of System Utilities	01.t – Session Time-out
01.j* - User Authentication for External Connections	01.y – Teleworking	01.u – Limitation of Connection Time
01.m* - Segregation in Networks	02.a* - Roles and Responsibilities	02.b – Screening
01.n* - Network Connection Control	03.a* - Risk Management Program Development	02.c – Terms and Conditions of Employment
01.o* - Network Routing Control	03.d – Risk Evaluation	02.d – Management Responsibilities
01.q* - User Identification and Authentication	04.a* - Information Security Policy Document	02.f* - Disciplinary Process
01.r* - Password Management System	05.a* - Management Commitment to Information Security	02.g – Termination or Change Responsibilities

CSF Controls – Most Relevant	CSF Controls –Relevant (Requires Further Analysis)	CSF Controls – Least Relevant
01.v* - Information Access Restriction	05.b* - Information Security Coordination	02.h – Return of Assets
01.w* - Sensitive System Isolation	05.f – Contact with Authorities	04.b* - Review of the Information Security Policy
01.x* - Mobile Computing and Communications	05.g – Contact with Special Interest Groups	05.c – Allocation of Information Security Responsibilities
02.e* - Information Security Awareness, Education and Training	05.i* - Identification of Risks Related to External Parties	05.d – Authorization Process for Information Assets and Facilities
02.i* - Removal of Access Rights	05.k* - Addressing Security in Third Party Agreements	05.e – Confidentiality Agreements
03.b* - Performing Risk Assessments	06.b – Intellectual Property Rights	05.h – Independent Review of Information Security
03.c* - Risk Mitigation	06.f – Regulation of Cryptographic Controls	05.j – Addressing Security When Dealing with Customers
06.d* - Data Protection and Privacy of Covered Information	06.j – Protection of Information Systems Audit Tools	06.a – Identification of Applicable Legislation
06.e* - Prevention of Misuse of Information Assets	07.c* - Acceptable Use of Assets	06.c – Protection of Organizational Records
06.g* - Compliance with Security Policies and Standards	07.d – Classification Guidelines	06.i – Information System Audit Controls
06.h – Technical Compliance Checking	07.e – Information Labeling and Handling	07.b – Ownership of Assets
07.a* - Inventory of Assets	08.j* - Equipment Maintenance	08.a – Physical Security Perimeter
*09.b*** - Change Management*	08.l* - Secure Disposal or Re-use of Equipment	08.b* - Physical Entry Controls
09.j* - Controls against Malicious Code	09.c*- Segregation of Duties	08.c – Securing Offices, Rooms and Facilities
09.k – Controls Against Mobile Code	09.d – Separation of Development, Test and Operational Environments	08.d* - Protecting Against External and Environmental Threats
*09.l*** - Back-up*	09.h – Capacity Management	08.e – Working in Secure Areas
09.m* - Network Controls	09.o* - Management of Removable Media	08.f – Public Access, Delivery and Loading Areas

CSF Controls – Most Relevant	CSF Controls –Relevant (Requires Further Analysis)	CSF Controls – Least Relevant
*09.n** - Security of Network Services*	09.w – Interconnected Business Information Systems	08.g – Equipment Siting and Protection
09.q* - Information Handling Procedures	10.c – Control of Internal Processing	08.h – Supporting Utilities
09.s* - Information Exchange Policies and Procedures	10.e – Output Data Validation	08.i – Cabling Security
09.v – Electronic Messaging	10.g – Key Management	08.k – Security of Equipment Off-premises
09.x – Electronic Commerce Services	10.l* - Outsourced Software Development	08.m – Removal of Property
09.y – On-line Transactions	11.d – Learning from Information Security Incidents	09.a – Documented Operations Procedures
09.aa* - Audit Logging	11.e – Collection of Evidence	09.e* - Service Delivery
09.ab* - Monitoring System Use	12.a – Including Info. Security in the Business Continuity Mgmt. Process	09.f* - Monitoring and Review of Third Party Services
09.ac* - Protection of Log Information	12.b – Business Continuity and Risk Assessment	09.g* - Managing Changes to Third Party Services
09.ad – Administrator and Operator Logs	12.e – Testing, Maintaining and Reassessing Business Continuity Plans	09.i – System Acceptance
09.ae – Fault Logging		09.p* - Disposal of Media
09.af* - Clock Synchronization		09.r – Security of System Documentation
10.a – Security Requirements Analysis and Specification		09.t – Exchange Agreements
10.b* - Input Data Validation		09.u – Physical Media in Transit
10.f* – Policy on the Use of Cryptographic Controls		09.z – Publically Available Information
10.h* - Control of Operational Software		10.d – Message Integrity
*10.k*** - Change Control Procedures*		10.i – Protection of System Test Data
10.m* - Control of Technical Vulnerabilities		10.j – Access Control to Program Source Code
11.a* - Reporting Information Security Events		12.d – Business Continuity Planning Framework
11.b – Reporting Security Weaknesses		

CSF Controls – Most Relevant	CSF Controls –Relevant (Requires Further Analysis)	CSF Controls – Least Relevant
11.c* - Responsibilities and Procedures		
12.c* - Developing & Implementing Continuity Plans Incl. Info. Security		

* - Control required for CSF 2013 (v5) Certification

** - Control proposed for Certification in the mid-2013 CSF release (v5.1) (text also italicized)

*** - Control proposed for CSF 2014 (v6) Certification (text also italicized)

Bold Text – Controls deemed critical to cybersecurity but have not been identified for future inclusion in the controls required for CSF Certification

The initial set of fifty (50) "critical" cybersecurity controls identified in the first column of the table includes thirty-seven (37) controls already required for 2013 certification, one (1) control identified for certification with the upcoming mid-2013 CSF release, and three (3) controls identified for certification in 2014. Nine (9) controls are not currently being considered as a certification requirement.

The assignment of these controls will be vetted by a working group of representatives from various healthcare organizations at the HITRUST 2013 annual conference and published for public comment. The approved set of controls will also be made available for targeted assessment of an organization's relative state of cyber security preparedness through MyCSF later in 2013.

Q4. Are some of these practices not applicable for business or mission needs within particular sectors?

HITRUST believes all the controls of interest by NIST apply to healthcare; however, as noted through the cross reference between the practices and HITRUST Certification requirements, not all are equally important. Healthcare requires guidance on prioritizing security due to the technical and resource constraints most organizations in this industry face—everything cannot be done at once. This is fundamentally why HITRUST has prioritized certain requirements for certification over other requirements in the CSF. Practices including encryption and key management, identification and authorization of users, mission/system resiliency, and privacy and civil liberties protection should be prioritized in healthcare over the other security and privacy practices.

Q5. Which of these practices pose the most significant implementation challenge?

Security engineering arguably presents the most significant implementation challenge for most healthcare organizations, especially small healthcare providers. Even relatively non-technical engineering-related controls such as change control / configuration management and information technology project management can be difficult for most organizations to implement properly. Identification and authentication of users also poses a challenge for most healthcare providers due to patient safety and other concerns.

Q6. How are standards or guidelines utilized by organizations in the implementation of these practices?

As noted in responses to previous questions, the HITRUST CSF aligns with most of the security practices listed. Each of these controls includes between one and three levels of implementation requirements, which define the detailed policies, processes and technologies that organizations must put in place in order to comply with the control, or in this case meet the practice. Additional sections for segment-specific requirements are also provided.

With the certification criteria, organizations leverage the questions developed by HITRUST that align with the controls required in the CSF in order to evaluate either their compliance with the requirements or their maturity (using a PRISMA-based scale) depending on the needs of the organization. The compliance assessment provides a gap analysis that organizations can use to ensure the control requirements are implemented. The maturity assessment, when used in conjunction with control-level impact ratings, allows organizations to make judgments about relative risk, support the selection of risk treatments, and prioritize remediation activities. Organizations also use share this information with regulators, business partners, business associates and other third parties to provide assurances around their information protection programs.

Q7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

With respect to budgeting, HITRUST requires that organizations ensure all capital planning and investment requests include the resources needed to implement the information security program, document all exceptions for this requirement; and ensure all resources are available for expenditure as planned.

Unfortunately gaining the resources needed is a considerable constraint for many healthcare organizations. This is highlighted in a 2009 Life Sciences and Health Care Study by Deloitte, which cited "budget constraints and/or lack of resources" as the predominant barrier to implementing IT security for Providers (59.18% of respondents noted this as an issue). When looking at the allocation of budgets compared with IT, Deloitte found that "67% of respondents indicate that less than 10% of their overall IT budget is dedicated to information security. This is consistent with the finding that security budgets are not keeping pace because security is not getting a high enough percentage of the overall IT budget."

While a process may exist to allocate resources for IT security, in healthcare the lack of support and adequate funding is a challenge that must still be overcome.

Q8. Do organizations have a formal escalation process to address cyber security risks that suddenly increase in severity?

HITRUST requires that formal information security event reporting procedures to support the corporate direction (policy) be established, together with an incident response and escalation procedure, to set out the action to be taken on receipt of a report of an information security event, treating the breach as discovered, and ensure the timeliness of reporting and response. The requirements also specify that a point of contact be established for the reporting of information security events.

In addition, the HITRUST C3 relies upon a community defense approach to support the industry's preparedness and response to cyber threats and attacks. It facilitates early identification, coordinated response and incident tracking, as well as knowledge sharing and enhanced preparedness for healthcare organizations challenged by cyber attacks. The center is focused on cybersecurity threats and events targeted at healthcare organizations in areas, including, but not limited to, networks, mobile devices, workstations, servers, applications and medical devices.

The center is also working with the U.S. Department of Health and Human Services to timely share various incident information and for participation in the Critical Infrastructure Information Sharing and Collaboration Program (CISCP). This sharing of information is crucial for organizations' preparedness, protection and crisis management.

Also available through HITRUST C3 is the HITRUST Cyber Threat Analysis Service (CTAS), which aims to help healthcare organizations prioritize their cybersecurity efforts and raise security awareness by informing them of general and sector-specific threats impacting the industry.

Q9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

Threats to data quality and privacy already abound with implementation of electronic health records (EHRs) and health information exchanges (HIEs) at the local, state and national levels. A voluntary set of information protection safeguards that address the implementation of these practices will help organizations mitigate these specific threats. HITRUST perceives the privacy and civil liberties' risks associated with their implementation as minimal given that, for the most part, PHI need not be divulged.

Q10. What are the international implications of this framework on your global business or in policymaking in other countries?

Given the international scope of the HITRUT CSF and CSF Assurance Program from the widespread use of "off-shore" business associates, the adoption of a common cyber-security framework will only improve acceptance of the CSF and other compliant information protection frameworks by these entities. A common framework within the U.S. would also help drive acceptance and similar policy-making in other countries that provide significant third-party support to U.S. healthcare and other industries providing critical infrastructure.

Q11. How should any risks to privacy and civil liberties be managed?

As stated, HITRUST does not believe a common cybersecurity framework will present additional risks to privacy and civil liberties. A component of privacy is the ability to identify and implement security controls effectively. In healthcare, the HIPAA Privacy Rule demonstrates this through the standard 164.530(c)(1) which states that "a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." NIST has similarly recently integrated privacy requirements into SP 800-53, expanding its scope to both privacy and security as opposed to just security. HITRUST is following suit based on these changes and the requests of the healthcare industry to integrate these two components, privacy and security, into a single framework of controls that incorporates the HIPAA Privacy Rule, NIST 800-53 r4 Appendix J Privacy Control Catalog, AICPA Generally Accepted Privacy Principles, state requirements and other sources as applicable. This will allow the privacy and security functions in healthcare organizations to better coordinate their initiatives and achieve the same goals of protecting sensitive health information.

HITRUST recommends a cyber security framework that applies to all industries, but at the very least within healthcare, incorporates both aspects of privacy and security to demonstrate the close relationship of these to concepts, and better safeguard sensitive systems and information through an integrated approach.

Q12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

Understanding what is specifically included in the core practices considered for the framework would allow commenters to provide more guided feedback; however, based on HITRUST's interpretation of the practices aligned with the CSF and more specifically HITRUST's initial selection of relevant cybersecurity controls, there may be a limited number of gaps that should be considered (only additional controls reflected):

Additional Practice for Consideration	Description
Information Protection Program	No additional controls
Endpoint Protection	09.j Controls Against Malicious Code
Portable Media Security	09.q Information Handling Procedures
Mobile Device Security	01.x Mobile Computing and Communications
Wireless Security	09.m Network Controls
Configuration Management	06.g Compliance with Security Policies and Standards
Vulnerability Management	10.b Input Data Validation
Network Protection	09.m Network Controls
Transmission Protection	09.s Information Handling Procedures
Password Management	No additional controls
Access Control	01.v Information Access Restriction 02.i Removal of Access Rights 06.e Prevention of Misuse of Information Assets

Audit Logging & Monitoring	09.ac – Protection of Log Information 09.af Clock Synchronization
Education, Training and Awareness	02.e Information Security Education, Training and Awareness
Third Party Assurance	No additional controls
Business Continuity & Disaster Recovery	No additional controls
Risk Management	03.b Performing Risk Assessments 03.c Risk Mitigation
Physical & Environmental Security	No additional controls

HITRUST believes that each of these additional topics represents either a common and fundamental component of compliance that applies broadly across all industries, and an area of significant risk whereby a lack of adequate protections in an error could result in a significant loss of sensitive information or the disablement of critical infrastructure (e.g., in healthcare, the inability to effectively treat patients).

HITRUST can provide additional comments on these and other controls that may be relevant to cybersecurity in the healthcare industry upon request.