HITRUST™

HITRUST CSF v9 Enhancements Extend "Assess Once, Report Many" Approach as a Standard Security Framework for Multiple Critical Infrastructure Industries

HITRUST CSF Certification now includes NIST Cybersecurity Certification

July 20, 2017 – Frisco, TX – HITRUST announced today specific details surrounding its version 9 (v9) of the HITRUST CSF, to be released in mid-August 2017. This release is a continuation of HITRUST's efforts to improve the overall state of information protection by providing organizations with a comprehensive, common approach to managing information privacy and security risks including those from cyber. The HITRUST CSF—the most widely adopted controls framework in the healthcare industry—is quickly developing as a standard in other industries and is gaining broader adoption internationally.

A driver behind this broader growth is found in HITRUST's support for an organization's attestation of compliance with the NIST Cybersecurity Framework (NIST CsF). With the release of HITRUST CSF v9, a single CSF assessment will include the controls necessary to address the NIST CsF requirements and an addendum to the HITRUST CSF Assessment report has been added to display the HITRUST CSF controls through the lens of the NIST CsF Core Subcategories.

"By incorporating the NIST Cybersecurity Framework into the HITRUST CSF and establishing a certification mechanism as part of the CSF Assurance program, organizations now have a effective and efficient approach for reporting an organization's cybersecurity posture leveraging the NIST Cybersecurity categorization," said Jason Newman, Vice President, Chief Information Security Officer, Blue Cross and Blue Shield of Minnesota. "This is another benefit in leveraging a common and comprehensive framework in the HITRUST CSF".

By increasing the number of HITRUST CSF controls required for HITRUST CSF Certification from 66 to 75, organizations will now be able to leverage a single risk assessment to obtain a standardized report against a common set of security and privacy controls for an "assess once, report many" approach for multiple industries beyond healthcare such as financial services and European markets. This includes assurances for how well an organization is meeting the objectives specified by the NIST Cybersecurity Framework Core Subcategories, Federal Financial Institutions Examination Council (FFIEC) Information Security Examination Handbook and the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria for Security, Confidentiality and Availability (including for SOC2 reporting), or support attestations of compliance with the HIPAA Security Rule.

To help organizations better leverage the HITRUST CSF and the CSF Assurance Program, regardless of their primary industry, the HITRUST CSF v9 release incorporates:

- **Federal Financial Institutions Examination Council (FFIEC) Information Security Examination Handbook**: The FFIEC IT Examination Handbook – Information Security was added as an authoritative source to improve use by financial organizations—most specifically those that provide their own health benefit—to make it easier for them to interpret the HITRUST CSF Assessment Report.
- **Federal Risk and Authorization Management Program (FedRAMP):** Given industry's increasing reliance on Cloud-based services, the incorporation of FedRAMP into the HITRUST CSF will allow organizations to identify a common set of controls for the provider and the consumer of these services, as well as support future guidance on their respective roles and responsibilities. HITRUST anticipates promulgating this type of guidance for Infrastructure as a Service (IaaS) providers in late 2017 and offering a targeted assessment and certification of IaaS providers based on this guidance in 2018.
- **Department of Homeland Security (DHS) Critical Resilience Review (CRR) cybersecurity criteria**: HITRUST users will also be able to use their existing HITRUST CSF-based information protection programs and associated assessments to provide general assurances around the state of their cybersecurity programs and level of organizational reliance based on the DHS CRR. This further enhances the common approach used by HITRUST to provide cybersecurity assurances via a NIST Cybersecurity Framework scorecard.
- **Office of Civil Rights' (OCR) Audit Protocol v2**: The HITRUST CSF v9 release also incorporates minor updates in the HITRUST CSF control requirements and associated assessment procedures based on a review of the Office of Civil Rights' (OCR) Audit Protocol v2. This helps ensure healthcare organizations can readily demonstrate compliance with the HIPAA Security Rule in the context of the Protocol for an OCR audit or in the event of a post-breach investigation.
- **Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11):** Coverage of Title 21, Code of Federal Regulations (CFR) Part 11 was also expanded to address Food and Drug Administration (FDA) requirements for electronic records as well as electronic signatures, which better supports organizations that must demonstrate FDA-compliance based on their HITRUST CSF-based information protection program.

By addressing this broad collection of regulatory requirements within the single, widely-accepted framework, the HITRUST CSF reduces the resources required to define, implement, and measure risk assessment programs across each of the regulations and standards that apply to an organization's specific needs.

"We are excited for the release of version 9 as it shows the continued evolution of the HITRUST CSF framework and program in addressing emerging information security risks. The framework continues to be critical in helping our clients and their various user organizations related to implementing an assess-once/report-many third-party assurance process, especially given that the framework is recognized as 'suitable criteria' for producing an AICPA SOC 2 report," said Scott Taylor, Partner, Deloitte & Touche LLP.

"Integration of the FFIEC information security requirements into the HITRUST CSF and CSF Assurance Program expands the framework's applicability and allows broader adoption in the financial services sector, as well as better context for those reviewing HITRUST CSF Assurance reports from third parties," said Dr. Bryan Cline, vice president, standards and analytics, HITRUST. "It's part of a concerted effort by HITRUST to evolve the HITRUST CSF into a more broadly and globally accepted framework that provides value for all types of industry."

HITRUST will be increasing its level of support for global organizational privacy programs in an interim v9.1 release of the HITRUST CSF by incorporating the European Union (EU) Regulation 2016/679, General Data Protection Regulation (GDPR), and mapping the HITRUST CSF's privacy and security requirements to the AICPA Trust Services Criteria for Privacy. These changes will increase applicability of the HITRUST CSF for privacy programs across multiple industries, both nationally and internationally. HITRUST anticipates v9.1 becoming available in February of 2018.

HITRUST, in consultation with the HITRUST CSF Advisory Council, actively solicits input from the industry on potential changes and updates to the framework, in addition to comments on changes implemented with each new release of the HITRUST CSF.

"HITRUST continues to be a leading voice for the health care industry on effective information security efforts, and these latest developments continue its history of helping the industry keep pace with a constantly changing environment," said Kirk Nahra, Partner, Wiley Rein LLP, privacy expert and member, CSF Advisory Council.

A more detailed explanation of the updates in the v9 release can be found in the HITRUST CSF v9 Summary of Changes, which will be included as part of the complete HITRUST CSF download upon release.

Helpful Links:

- The Healthcare Sector Cybersecurity Framework Implementation Guide from the Department of Homeland Security - Cybersecurity Framework Website
- The official press release for the HITRUST Threat Catalogue
- More information on the HITRUST CSF

For questions about the HITRUST CSF v9 updates, please feel free to contact HITRUST at info@hitrustalliance.net.

About HITRUST

Founded in 2007, the HITRUST Alliance, a not for profit, was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST—in collaboration with public and private healthcare technology, privacy and information security leaders—has championed programs instrumental in safeguarding health information and managing information risk while ensuring consumer confidence in the organizations that create, store or exchange their information.

HITRUST develops, maintains and provides broad access to its common risk and compliance management and de-identification frameworks, and related assessment and assurance methodologies, as well as programs supporting cyber sharing, analysis and resilience. HITRUST also leads many efforts in advocacy, awareness and education relating to information protection.

For more information, visit www.HITRUSTalliance.net.

###

Media Contacts: Leslie Kesselring
Kesselring Communications for HITRUST leslie@kesscomm.com or pr@HITRUSTalliance.net
+1 503 358 1012