HITRUST

HITRUST Announces HITRUST CSF Roadmap Including a New Simplified Program for Small Healthcare Organizations and NIST Cybersecurity Framework Certification

Introducing HITRUST CSFBASICs and significant HITRUST CSF updates in 2017

March 1, 2017 – Frisco, TX: HITRUST announced today its 2017 roadmap for key enhancements to the HITRUST CSF as well as a new CSF initiative targeting smaller healthcare organizations to support their information risk management programs and improve their cyber resilience. The HITRUST CSF continues to be the most widely adopted information privacy and security framework that provides healthcare organizations with a comprehensive, scalable and certifiable approach to regulatory compliance and risk management. The 2017 roadmap demonstrates HITRUST's continued efforts to ensure the HITRUST CSF and CSF Assurance programs remain relevant and effective given the changing cyber threat and information risk landscape, as well as its leadership in advancing the state of information protection for the healthcare industry.

Being announced today:

- **CSFBASICs:** Streamlined versions of the HITRUST CSF and supporting HITRUST CSF Assurance Program designed to help small and lower-risk healthcare organizations meet otherwise difficult regulatory and risk management requirements.
- **HITRUST CSF V8.1:** Continued enhancements including support for PCI DSS v3.2 and MARS-E v2.
- **HITRUST CSF v9:** Continued enhancements including OCR Audit Protocol v2, FEDRAMP Support for Cloud and IaaS Service Providers and FFIEC IT Examination Handbook for Information Security.
- **CSF Assurance Program v9:** Enhanced so that a HITRUST CSF Assessment also includes a NIST Cybersecurity Framework certification with auditable documentation in addition to a HIPAA risk assessment.

HITRUST CSFBASICs Treats Small Healthcare Risk

In response to feedback from smaller healthcare organizations looking for a viable means to meet regulatory demands while protecting their business against cyber threats, HITRUST collaborated with the physician community and small businesses to develop and pilot a new program called CSFBASICs (*CSF Basic Assurance and Simple Institution Cybersecurity*). This program provides lower-risk organizations with a

simplified set of requirements and a streamlined assessment approach that is easier to understand and implement, and offers third parties—including regulators—appropriate assurances and transparency into their information privacy and security programs.

“I really don’t know many small practices that can comply with all our regulatory obligations, including HIPAA,” said Dr. J. Stefan Walker, physician, Corpus Christi Medical Associates (CCMA), a small five-physician primary care practice in Corpus Christi, Texas. “We generally don’t have the staff or the expertise, nor can we hire consultants, to manage these programs on an ongoing basis. I honestly didn’t know how my practice could be secure or demonstrate HIPAA compliance, but that was before I had the opportunity to pilot CSFBASICs.”

The CSFBASICs and CSFBASICs Assurance programs are currently in the final phase of piloting and are scheduled for general availability in Q3 2017.

HITRUST CSF and CSF Assurance Program Updates Deepen Assurance and Reduce Risk

The HITRUST CSF and CSF Assurance programs already provide the foundation for healthcare’s implementation of the NIST Cybersecurity Framework, and forms the basis for current Healthcare and Public Health (HPH) sector guidance. Given the increased risks associated with cyber threats and renewed focus on cyber resilience, HITRUST is further enhancing the CSF and CSF Assurance programs to provide better guidance, assurance and support to organizations, while encouraging a greater focus on cyber resilience within the industry.

“HITRUST is expanding the controls required for HITRUST CSF Certification, from 66 to no more than 75, to enhance its support for an organization’s certification of compliance with the NIST Cybersecurity Framework,” said Dr. Bryan Cline, vice president, standards and analytics, HITRUST. “CSF Certified organizations will be able to provide both HIPAA and NIST Cybersecurity Framework compliance scorecards based on a single CSF assessment, which are incorporated into the HITRUST CSF Assessment Report.”

To help ensure continued efficacy and relevancy, 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 those changes implemented with each new release of the HITRUST CSF. The recent creation of the HITRUST Threat Catalogue will further enhance the underlying risk analyses used to develop the HITRUST CSF and help ensure the HITRUST CSF and CSF Assurance Program continue to remain current and relevant in a heightened threat environment.

HITRUST

There are two HITRUST CSF releases scheduled in 2017. A minor release—CSF v8.1—that was made available on February 6, 2017, and a major release—CSF v9—which is scheduled for July 2017. Among several minor enhancements, the HITRUST CSF v8.1 release updates content and mappings for PCI DSS v3.2 and MARS-E v2. A more detailed explanation of the updates in the v8.1 release can be found in the HITRUST CSF v8.1 Summary of Changes (included as part of the complete HITRUST CSF download).

With the v9 release targeted for July, HITRUST will ensure relevant CSF control requirements are aligned with language in the second release of the Office for Civil Rights (OCR)'s Audit Protocol. Given the healthcare industry's increasing reliance on the Cloud, FedRAMP requirements will also be incorporated. The intent is to provide guidance to providers and consumers of Infrastructure as a Service (IaaS) offerings on roles and responsibilities for HITRUST CSF control requirements, and support a targeted assessment and certification approach for IaaS providers.

Other authoritative sources to be added to v9 include the Federal Financial Institutions Examination Council's IT Examination Handbook – Information Security requirements, in order to improve use by organizations outside of healthcare; the Department of Homeland Security's Cyber Resilience Review (CRR), in order to further support its foundational role in healthcare's implementation of the NIST Cybersecurity Framework; and the HITRUST Threat Catalogue, which will be fully integrated with v10 in 2018.

Because HITRUST recognizes that the need to integrate additional authoritative sources potentially increases the complexity of the framework and the assessments conducted against it, the alliance is also working diligently to further harmonize these requirements in future releases including v9. By continuing to consolidate and streamline these requirements in the HITRUST CSF, HITRUST CSF assessments will continue to provide the most robust, efficient and cost-effective levels of assurance.

Helpful Links:

- The HITRUST CSF v8.1 Summary of Changes (included as part of the complete HITRUST CSF download)
- The Healthcare Sector NIST 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 v8.1 updates contact HITRUST at info@hitrustalliance.net.

HITRUST

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