HITRUST CSF®

Version 9.4.2 Summary of Changes

Incorporates changes stemming from the integration of the U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC) Framework and NY DOH Office of Health Insurance Programs SSP v3.1 Authoritative Sources.

December 2020

HITRUST®

Fundamental to HITRUST's mission is the availability of a common security and privacy framework, the HITRUST CSF ("CSF"), which provides the needed structure, transparency, guidance, and cross-references to authoritative sources organizations globally need to be certain of their data protection compliance. The initial development of the CSF leveraged nationally and internationally accepted security and privacy related regulations, standards, and frameworks—including ISO, NIST, PCI, HIPAA, and COBIT—to ensure a comprehensive set of security and privacy controls. The CSF standardizes these requirements, providing clarity and consistency and reducing the burden of compliance.

In developing a framework that can meet the needs of organizations locally, nationally, and globally, HITRUST recognizes that various organizations may have requirements imposed as a result of being part of a smaller community—such as a subset of an industry group or by a cooperative sharing agreement. In many cases, these may not be new security or privacy controls but more specific implementation requirements. HITRUST provides the capability for these requirements to be incorporated, harmonized, and selected for inclusion during the assessment process and then included in the HITRUST CSF Assessment Report, utilizing the MyCSF platform. The intent is to reduce any additional assessments by enabling organizations to Assess Once, Report Many™. The HITRUST CSF now includes such community-specific authoritative sources, currently referred to as supplemental requirements (SR) or community supplemental requirements (CSR). Organizations required or choosing to include community-specific authoritative sources may select them with other regulatory factors under the Admin & Scoping section of the MyCSF platform. HITRUST continues to evaluate the inclusion of others based on market demand.

HITRUST ensures the CSF stays relevant and current to the needs of organizations by regularly updating the CSF to integrate and normalize applicable requirements and best practices as authoritative sources and community supplemental requirements.

This release includes changes based on feedback from the HITRUST community, miscellaneous corrections, incorporation of Department of Defense (DoD) Cybersecurity Maturity Model (CMMC) Framework version 1.0 and NY DOH Office of Health Insurance Programs SSP v3.1 authoritative sources. These updates reflect HITRUST's commitment to provide a framework fitting for any organization globally. Minor administrative updates, such as the correction of grammar or formatting errors, are generally not reflected in the Summary of Changes.

The table below provides a summary of the changes to the CSF broken down by Control Reference and Implementation Requirement Level.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
00.a	CMMC	Added: The organization establishes, maintains, and resources: an access control plan with a focus on: i) establishing system access requirements, ii) controlling internal system access, iii) controlling remote system access, and iv) limiting data access to authorized users and processes; an asset management plan with a focus on: i) identifying and documenting assets, ii) managing the asset inventory, iii) defining audit requirements, iv) performing audits, v) identifying and protecting audit information, and vi) reviewing and managing audit logs; an audit and accountability plan with a focus on: i) defining audit requirements, ii) performing audits, iii) identifying and protecting audit information, and iv) reviewing and managing audit logs; an awareness and training plan with a focus on: i) conducting security awareness activities, and ii) conducting training; a configuration management plan with a focus on: i) establishing configuration baselines, and ii) performing configuration and change management; an identification and authentication plan with a focus on granting access to authenticated entities; an incident response plan with a focus on: i) planning incident response, ii) detecting and reporting events, iii) developing and implementing a response to a declared incident, iv) performing post incident reviews, and v) testing incident response;	Necessitates new Implementation Language. Continued on next page.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
00.a	CMMC	a maintenance plan with a focus on managing maintenance; a media protection plan with a focus on: i) identifying and marking media, ii) protecting and controlling media, iii) sanitizing media, and iv) protecting media during transport; a personnel security plan with a focus on: i) screening personnel, and ii) protecting CUI during personnel actions; a physical protection plan with a focus on limiting physical access; a recovery plan with a focus on: i) managing backups, and ii) managing information security continuity; a risk management plan with a focus on: i) identifying and evaluating risk, ii) managing risk, and iii) managing supply chain risk; a security assessment plan with a focus on: i) developing and managing a system security plan, ii) defining and managing controls, and iii) performing code reviews; a situational awareness plan with a focus on implementing threat monitoring; a system and communications protection plan with a focus on: i) defining security requirements for systems and communications, and ii) controlling communications at system boundaries; and a system and information integrity plan with a focus on: i) identifying and managing information system flaws, ii) identifying malicious content, iii) performing network and system monitoring, and iv) implementing advanced email protections.	Continued from prior page.
01.d	Supplemental Requirements	Added: Authentication credentials are provided using a secure method.	Necessitates new Implementation Language.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
01.j	CMMC	Added: The system restricts remote network access based on organizational defined risk factors, e.g., time of day, location of access, physical location, network connection state, and measured properties of the current user and role.	Necessitates new Implementation Language.
01.n	CMMC	Added: The organization uses encrypted sessions for the management of network devices.	Necessitates new Implementation Language.
01.o	Community Supplemental Requirements 002	Added: The system i) routes Internet traffic through a network intermediary device such as a content-filtering proxy server; ii) prevents end-user systems from communicating directly to the Internet; iii) does not solely rely on host-based controls to route Internet traffic; iv) inspects encrypted Internet traffic; v) uses reputation service to maintain an updated list suspicious domains and URL strings; vi) blocks malicious content, high-risk websites, and uncategorized websites; and vii) analyzes traffic based on more criteria than domain name or IP, including URL, GETs, POSTs, content types (e.g. Flash), and user-agents.	Necessitates new Implementation Language.
01.o	CMMC	Added: The organization defines and employs tailored network boundary protections in addition to implementing commercially available solutions.	Necessitates new Implementation Language.
01.q	Community Supplemental Requirements 002	Added: The organization requires the use of multifactor authentication for privileged access to administrative network zones. The organization manages access to all shared privileged accounts such that individual accountability are preserved and credentials are not synchronized across environments.	Necessitates new Implementation Language.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
01.q	Supplemental Requirements	Added: Maintain individual ownership and accountability for use of all service accounts.	Necessitates new Implementation Language.
01.t	Supplemental Requirements	Added: A time-out mechanism (e.g., screensaver) pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed.	Necessitates new Implementation Language.
01.v	1	Updated: Access rights to applications and application functions ~~are limited to the minimum necessary using menus.~~ should be restricted in accordance with the access control policy.	Implementation Language updated to provide further clarity and alignment with the authoritative source(s).
03.b	CMMC	Added: The organization analyzes the effectiveness of security solutions at least annually to address anticipated risk to the system and to the organization based on current and accumulated threat intelligence.	Necessitates new Implementation Language.
05.g	FedRAMP	Updated: The organization receives information system security alerts, advisories, and directives ~~from US-CERT~~ on an ongoing basis. Furthermore, the organization generates and disseminates security alerts, advisories, and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities; and implements security directives in accordance with established time frames or notifies the business owner of the degree of noncompliance.	Implementation Language updated to provide further clarity and alignment with the authoritative source(s).

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
05.i	Community Supplemental Requirements 002	Added: The organization performs due diligence on incident management service providers to ensure the provider has a credible history and is capable of providing the necessary services, and re-evaluates the capabilities on a regular basis (e.g., prior to contract renewal).	Necessitates new Implementation Language.
05.k	Community Supplemental Requirements 002	Added: The organization executes service contracts for incident management through an outside legal party to ensure client/attorney confidentiality.	Necessitates new Implementation Language.
05.k	Supplemental Requirements	Added: Supplier complies to requirements under the supplier agreement, including maintaining and adhering to documented processes for (i) reviewing and scanning software developed or customized for the organization to find and remediate malicious code and/or security vulnerabilities prior to initial deployment, and making scan results and remediation plans available to the organization upon request; (ii) cooperating with the organization and taking all reasonable and necessary steps to isolate, mitigate, terminate, and/or remediate all known or suspected threats within 90 days of notification of a threat to the organization or its customers' nonpublic information resources originating from the supplier's network; and (iii) notifying and cooperating with the organization upon discovery of a supplier's noncompliance with the organization's security requirements, or of a known or suspected threat/vulnerability impacting the organization or its customers, and to take all reasonable and necessary steps to isolate, mitigate, and/or remediate such noncompliance or threat/vulnerability within 90 days. Supplier maintains and adheres to any business continuity plan and/or disaster recovery plan requirements under the agreement.	Necessitates new Implementation Language.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
06.a	2	Updated: The organization joins industry trade associations, subscribes to thought leadership and market/security research organizations, or establishes some other reliable process to stay abreast of business sector, industry, technology, infrastructure, and legal and regulatory environment trends that may impact the organization's security policies; and the consequences of these impacts are incorporated into the development or update of the organization's policies and procedures.	Implementation Language updated to provide further clarity and alignment with the authoritative source(s).
06.c	Supplemental Requirements	Added: Guidelines are issued by the organization on the ownership, classification, retention, storage, handling, return, and disposal of all records and information. Separation between operational information and non-production (development, test/quality assurance) environments is maintained. The organization maintains controls to detect and terminate unauthorized attempts to access, modify, store, and/or handle in-scope information. The confidentiality and integrity of information is protected at rest and in transit in the following scenarios using a cryptographic algorithm with minimum key lengths of 256 bits for symmetric and 2048 bits for asymmetric, and proper key management practices including keys with a maximum lifetime of two years for: (i) all in-scope information (ISI) transmitted over untrusted networks; (ii) all ISI stored or transmitted using mobile and portable devices; (iii) all wireless networking technologies used to transmit ISI; (iv) all ISI stored within, or transmitted to, from, and within non-organizational cloud services; and (v) all sensitive personal information (SPI)/sensitive customer data (SCD) stored or transmitted over all networks, including trusted networks.	Necessitates new Implementation Language.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
06.d	Group Health Plans	Updated: Group Health Plan plan documents incorporate provisions to require the plan sponsor to: i) implement administrative, physical, and technical safeguards to reasonably and appropriately protect electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan; ii) ensure that adequate separate is supported by reasonable and appropriate security measures; iii) ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and iv) report to the group health plan any security incident of which it becomes aware.	Requirement Statement updated to provide further clarity and alignment with the authoritative source.
06.d	HIPAA	Updated: Workstations that can access electronic protected health information are configured with specifications that address: i) proper functions to be performed, ii) the manner in which those functions are to be performed, and iii) physical attributes of the surroundings.	Requirement Statement updated to provide further clarity and alignment with the authoritative source.
06.f	CMMC	Added: The organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards when used to protect the confidentiality of information.	Necessitates new Implementation Language.
09.d	Supplemental Requirements	Added: Separation between production and non-production (development, test/quality assurance) environments is established and controls are implemented to prevent operational issues.	Necessitates new Implementation Language.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
09.e	Community Supplemental Requirements 002	Added: The organization executes a master service agreement with a third-party service provider experienced in incident response and forensics on a contingency basis. The organization ensures that service contracts for incident management require the service provider to deliver immediate remote support and be on-site (if possible and/or where practical) within 48 hours of an incident.	Necessitates new Implementation Language.
09.f	Supplemental Requirements	Added: Supplier (i) ensures all supplier entities performing any in-scope work are contractually obligated to comply with the organization's security requirements, or requirements that are no less stringent; (ii) ensure the use of the organization's information resources and in-scope information by supplier entities will only be for the performance of in-scope work; (iii) maintain and adhere to a documented program by which supplier entity compliance to the organization's security requirements is evaluated by supplier and all corrective actions are documented and implemented; and (iv) upon the organization’s request, supplier will provide documentation and/or evidence to adequately substantiate such compliance.	Necessitates new Implementation Language.
09.h	Supplemental Requirements	Added: The organization protects against or limits the effects of various types of denial-of-service attacks, including distributed denial-of-service attacks.	Necessitates new Implementation Language.
09.j	CMMC	Updated: The organization employs advanced analytics (e.g., sandboxing) to test untrusted code and/or programs traversing through the network or system boundaries, in order to detect and block malicious content.	Implementation Language transferred from Control Reference 09.m to 09.j and updated to provide further clarity.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
09.j	Community Supplemental Requirements 002	Added: The organization augments endpoint protection strategies with additional solutions—including those built into the operating system if available—to mitigate exploitation of unknown vulnerabilities where traditional antivirus may be ineffective; and where applicable, target the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins).	Necessitates new Implementation Language.
09.m	CMMC	Updated: The organization uses encrypted sessions for the management of network devices.	Implementation Language transferred from 01.n to 09.m.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
09.m	Community Supplemental Requirements 002	Added: The organization utilizes a hardened intermediary system, running only a pre-defined set of applications (without Internet access or office productivity applications), to: i) prevent end-users from directly communicating to administrative network zones; and ii) control privileged access for administrators, developers, and others who need greater network access than regular end-users, to perform their job duties. The organization restricts communication with administrative network zones using a deny-by-default and allow-by-exception policy for all ports, protocols, and services, including the use of administrative interfaces from intentionally published services that may allow unauthorized information access. The organization protects workstations from potentially-compromised peers by: i) blocking inbound communication from other workstations to prevent network traffic between workstations (e.g., using host-based firewalls); and ii) allowing only communication from administrative services (e.g. configuration management, domain controllers, remote support systems). Exceptions are approved on a limited basis to specific sources and destinations. The organization develops a capability for capturing and retaining network traffic and/or network flows at key points in the network and between different trust zones to support dependent operational processes, while managing associated costs. The organization employs a mechanism to aggregate and retain network traffic flows (as appropriate, based on risks and regulations) in a searchable repository, which can be used to support alerting, response, investigation, and forensics processes, including reconstructing artifacts and indexing packet captures for analyses.	Necessitates new Implementation Language. Continued on next page.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
09.m	Community Supplemental Requirements 002	The system scans and inspects inbound payloads in its entirety, using sandboxing or malware detonation technologies to detect and block malicious content, prior to reaching endpoints. The system (i) controls the domain name system (DNS) infrastructure by using enterprise-managed DNS servers; (ii) systematically identifies and blocks traffic to malicious domain names (blackholing); and (iii) redirects blackholed domains to a non-routable address or other specified destination for monitoring.	Continued from prior page.
09.aa	Community Supplemental Requirements 002	Added: The organization implements a centralized mechanism to log privileged activities, including the use of privileged accounts and grants to privileged groups; and develops alerting rules and investigation procedures to review suspicious activities.	Necessitates new Implementation Language.
09.ab	CMMC	Updated: The organization establishes and maintains a security operations center capability that facilitates 24/7 incident detection and response.	Implementation Language transferred from Control Reference 09.m to 09.ab.
10.a	CMMC	Added: The organization designs network and system security capabilities to leverage, integrate, and share Indicators of Compromise (IoC).	Necessitates new Implementation Language.
10.c	Community Supplemental Requirements 002	Added: The organization incorporates domain name system (DNS) blackholing into its incident detection and response procedures, including (i) generating alerts to security personnel on queries to resolve blackholed domains; (ii) ensuring blackholing can be done quickly, as part of incident containment and prevention; and (iii) integrating with threat intelligence and other threat indicator sources to pre-emptively blackhole domains.	Necessitates new Implementation Language.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
10.h	CMMC	Added: The organization utilizes an exception process for non-whitelisted software that includes mitigation techniques.	Necessitates new Implementation Language.
10.m	Supplemental Requirements	Added: Maintain and adhere to a documented process to remediate all critical, high, and medium risk security vulnerabilities promptly.	Necessitates new Implementation Language.
11.c	CMMC	Added: The organization establishes and maintains a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours.	Necessitates new Implementation Language.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
11.c	Community Supplemental Requirements 002	Added: The organization develops incident detection and response procedures that include: i) identifying and alerting on anomalous network traffic (from lessons learned from investigations, variances to normal traffic models, anomalous behavior and other attack patterns identified by threat-hunting/data analysis); and ii) analyzing network packets to support investigation and forensics activities. The organization develops incident response plans that include the roles and responsibilities of both internal resources and third-party service providers, including details on when third-party service providers are required to assist in investigation and response activities. The organization develops a procedure to quarantine compromised systems and systems suspected of compromise to preserve evidence for investigation, and allows such systems only basic connectivity to other systems for response purposes. For host-based quarantine methods, the organization implements a process to determine whether the method failed to achieve intended results, and implements additional controls to isolate or remove from the network. The organization employs the capability to acquire system data in near real-time (remotely and directly) for deep forensic analysis. The organization employs the capability to actively search all deployed endpoints to readily identify threat indicators (e.g. from investigations or separate intelligence source). The organization keeps compromised systems in quarantine until the incident is fully remediated.	Necessitates new Implementation Language. Continued on next page.
11.c	Community Supplemental Requirements 002	The organization is inclined towards re-imaging a compromised system when there has been confirmed execution of potentially malicious code; otherwise, the organization uses caution when cleaning such systems to ensure malicious code is fully eradicated.	Continued from prior page.

CSF Control Reference	Requirement Level	Summary of Changes	Remarks
11.e	CMMC	Added: The organization establishes and maintains a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours.	Necessitates new Implementation Language.
11.e	Community Supplemental Requirements 002	Added: The organization deploys a solution to monitor and retain detailed endpoint telemetry that: i) records details such as trace of process execution (e.g. file paths, libraries called, sockets opened, files opened/written), network connections, file input/output, and registry changes; ii) can implement customized detection rules to complement endpoint preventative controls and address gaps in other solutions (e.g. banning files/hashes, network connections, processes execution); and iii) aggregates and makes data available to others for building detection rules and investigating incidents. The organization documents details on flow of sensitive data to the individual systems, including the details on system type (e.g., manufacturer, operating system), roles (e.g., database, file server), and network location (e.g., subnet, IP address).	Necessitates new Implementation Language.
12.a	HIPAA	Updated: The organization implements procedures under the disaster recovery plan (or related plans) to allow facility access in support of restoration activities in emergency-related events.	Requirement Statement updated to provide further clarity and alignment with the authoritative source.