Aug 18, 2023

Appendix Governing Electronic Access to CHIPS

I. Scope

1.1 This appendix supplements the CHIPS Rules and sets forth terms governing the establishment and use of Electronic Access Methods to send data to and receive data from TCH in connection with the use of CHIPS.

1.2 TCH offers two Electronic Access Methods in connection with CHIPS. Each Electronic Access Method is more fully described in TCH Technical Specifications.

1.3 By establishing an Electronic Access Method, each Customer agrees to comply with the terms of this appendix and the requirements set forth in the applicable TCH Technical Specifications, as such terms and requirements are amended from time to time. In the event of any inconsistency between this appendix and the CHIPS Rules, the CHIPS Rules control.

II. Definitions

2.1 Access Control Feature means encryption keys, logon identifications, passwords, pass phrases, digital certificates, virtual private network devices, routers, removable certificate storage devices, personal identification numbers, encryption technology, workstation configurations, workstation or network access restrictions (physical or logical), and other security measures used for access, authentication, or authorization with regard to an Electronic Access Method.

2.2 CHIPS Rules means the CHIPS Rules and Administrative Procedures.

2.3 Customer means a CHIPS Participant as defined in the CHIPS Rules or a depository institution that is eligible to be a CHIPS Participant under the CHIPS Rules and seeks to establish or utilize an existing Electronic Access Method in order to become a CHIPS Participant.

2.4 Electronic Access Method refers to a multiprotocol label switching network, a virtual private network, the public internet, or other electronic connection used to exchange data between a Customer and TCH for which access, authentication, or authorization is controlled by use of one or more Access Control Features.

2.5 Malware means hardware, software, or firmware that is intentionally included or inserted in a system to affect the confidentiality, integrity, or availability of a system.

2.6 Security Event means an operational issue, cyber event, fraud, malware, compromise, or other security incident or breach that relates to or indicates it would affect an Electronic Access Method, Access Control Feature, or the use of CHIPS.

2.8 TCH Technical Specifications means the technical requirements and standards that TCH makes available to Customers in relation to CHIPS, as those requirements or standards are promulgated by TCH from time to time.

III. Prior Approval to Use Electronic Access Methods

3.1 A Customer shall not access, or attempt to access, any test or production environment established by TCH in connection with CHIPS without obtaining TCH's prior approval. Before a Customer uses a specific Electronic Access Method for or in relation to any transaction or other activity in the test or production environment for CHIPS, TCH and the Customer will determine which Electronic Access Method is appropriate and TCH will inform the Customer of any required testing. A Customer may not use an Electronic Access Method for transactions or other activity in any test or production environment established by TCH in connection with CHIPS until the Customer successfully completes all testing TCH has required.

IV. Hardware, Software, and Other Electronic Access Method Configuration Requirements

4.1 TCH Technical Specifications provide the specific hardware, software, and Access Controls Features required for each Electronic Access Method available for use in connection with CHIPS.

4.2 TCH may specify third-party suppliers through which a Customer must obtain hardware or software necessary for establishing and maintaining an Electronic Access Method.

4.3 With respect to hardware and software necessary for maintaining an Electronic Access Method each Customer is responsible for (a) ensuring that its computers and associated hardware and software comply with requirements in Technical Specifications provided by TCH (which TCH may change from time to time) and (b) maintaining its own computers, associated hardware, and software.

4.4 TCH may arrange for the delivery, installation, repair or alteration of TCH-supplied or -designated equipment necessary for establishing an Electronic Access Method. TCH-supplied or -designated equipment may not be altered, encumbered, relocated, removed, or transferred to a third party except with TCH's prior written approval. The Customer is liable for any loss of or damage to TCH-supplied or -designated equipment, ordinary wear and tear excepted. Notwithstanding that TCH may facilitate the delivery, installation, repair, or alteration of any equipment, TCH shall not assume any financial obligation or liability in connection with such delivery, installation, repair, or alteration, even if TCH required that such equipment be used in order to establish an Electronic Access Method.

4.5 With respect to an Electronic Access Method, a Customer shall not:

(a) modify, add to, translate, reverse assemble, reverse compile, decompile, or otherwise attempt to derive the source code from any software;

(b) copy, sublicense, or transfer the software for any reason, except that software may be copied for backup, testing, or archival purposes;

(c) remove any copyright or trademark notice contained in the software; or

(d) use any software or hardware for purposes other than the purpose for which it was provided.

4.6 When a Customer's participation in CHIPS is terminated, the Customer shall promptly follow TCH's instructions regarding all TCH-supplied or -designated equipment.

4.7 TCH may charge fees for an Electronic Access Method, including the use of TCH-supplied or -designated hardware, as set forth in a written pricing schedule.

V. Location of Customer Endpoints

5.1 A Customer shall not, except with TCH's prior written consent:

(a) situate any TCH-provided router used in conjunction with an Electronic Access Method in any location outside the United States, including its territories, to connect to CHIPS; or

(b) use an Electronic Access Method from outside the United States, including its territories, to connect to CHIPS, except as provided in section 5.3.

5.2 To the extent TCH grants consent to a Customer in connection with acts otherwise prohibited under section 5.1, TCH may subject the Customer's use of an Electronic Access Method to additional terms, including terms addressing the application of foreign data privacy laws.

5.3 A Customer may access the secure sockets layer virtual private network that connects Customers to CHIPS Web applications from outside the United States, subject to any controls TCH may implement for connections originating from countries that TCH deems high risk.

VI. Use of Access Control Features

6.1 A Customer:

(a) shall use all Access Control Features required by TCH in TCH Technical Specifications,

(b) shall ensure access to the Electronic Access Methods and Access Control Features is logically and physically restricted to authorized individuals, as specified in TCH Technical Specifications;

(c) is responsible for unauthorized physical and network access to the Electronic Access Methods and Access Control Features; and

(d) shall establish, institute, and enforce policies and procedures for controlling, detecting, and preventing unauthorized logical and physical access to all Access Control Features and Electronic Access Methods, as specified in TCH Technical Specifications.

6.2 TCH may act on any communication or data it receives through an Electronic Access Method.

VII. Maintenance of Electronic Access Methods

7.1 Each Customer shall manage each Electronic Access Method it uses so as to permit TCH to send data to it and to permit the Customer to receive data from TCH on a timely basis at such times as TCH may direct. At a minimum, such times include the period during CHIPS' hours of operation.

7.2 Each Customer shall implement the resiliency measures TCH requires to support CHIPS and shall participate in contingency tests organized by TCH from time to time. Notwithstanding the above, each Customer is solely responsible for establishing its own business continuity and disaster recovery plans.

VIII. Security Obligations

8.1 Each Customer agrees that complying with the Access Control Features required by TCH for use of a specific Electronic Access Method does not relieve the Customer of its obligation and responsibility to exercise its own independent judgments about security and about additional measures or procedures needed to prevent fraud, unauthorized access, or other unauthorized use of Electronic Access Methods.

8.2 In addition to complying with the Access Control Features required by TCH for use of a specific Electronic Access Method and TCH Technical Specifications, each Customer shall take all commercially reasonable security measures in establishing an Electronic Access Method as circumstances may dictate over time and shall take all commercially reasonable security measures that are necessary to prevent fraud, unauthorized access, or other unauthorized use of an Electronic Access Method or that are necessary to prevent disruption to the operations of the computers, networks, systems, or software of TCH or other Customers.

8.3 As further specified in TCH Technical Specifications, each Customer shall implement technical, operational, managerial, and procedural controls designed to protect the security of its information technology ("IT") environment, including (i) systems (physical or virtual) and processes that are used to access CHIPS and related applications or to send or receive data over an Electronic Access Method or (ii) any ancillary systems (physical or virtual) and processes used by the Customer in connection with the systems and processes set forth in Section 8.3(i). At a minimum, such technical, operational, managerial, and procedural controls must be consistent with guidance provided by the Federal Financial Institutions Examination Council, including its guidance regarding Authentication and Access to Financial Institution Services and Systems.

8.4 As further specified in TCH Technical Specifications, a Customer shall take all commercially reasonable precautions and protections to prevent the introduction of Malware that might affect the confidentiality, integrity, or availability of the computers, networks, systems or software of TCH or other Customers. At a minimum, such precautions and protection must include the installation, operation, and proper configuration of commercially reasonable anti-Malware software. The Customer shall institute and/or reinforce procedural controls, such as the timely patching of hardware and software (including operating systems, applications, and firmware) and regular scanning/assessment of the enterprise environment for vulnerabilities and other exposures.

IX. Incident Notification and Assurance

9.1 Each Customer shall promptly notify TCH of any Security Event.

9.2 TCH may immediately terminate a Customer's Electronic Access Method if TCH, in its sole discretion, determines that continued use of the Electronic Access Method poses a risk to TCH or others. TCH may

suspend or disconnect a Customer's Electronic Access Method in the event that such access to TCH systems generates error conditions, causes denials or disruptions of TCH's systems, or appears to have been compromised. In the event of any such suspension or disconnection, the Customer shall cooperate with TCH to investigate, identify, and correct the issues that led to the suspension or disconnection.

9.3 TCH has the sole right to determine when a Customer may use an Electronic Access Method after TCH has suspended or disconnected the Customer's Electronic Access Method. Before TCH makes such a determination, TCH may require that the Customer undertake due diligence, including:

(a) performing actions substantively similar to those set forth in Schedule 1 to this Appendix – Technical Checklist, and

(b) meeting requirements substantively similar to those set forth in Schedule 2 to this Appendix – Assurance Requirements, including a certification from the Customer's chief information security officer (or equivalent officer) as to the actions the Customer has taken to remediate the issue that caused suspension or disconnection.

The Customer shall promptly furnish to TCH such information produced by that due diligence as TCH may reasonably request to aid in TCH's determination.

X. Knowledge of Noncompliance

10.1 TCH's knowledge of noncompliance by any Customer with one or more requirements set forth in this appendix does not constitute TCH's approval of such noncompliance. Any such noncompliance is solely at the risk of the Customer that has failed to fully comply with this appendix.

XI. TCH Liability

11.1 TCH's liability with respect to its operation of CHIPS, including with respect to the matters addressed in this appendix, is determined as set forth in the CHIPS Rules (including as supplemented by this appendix).

XII. TCH Audit Rights

12.1 TCH maintains the right to audit, monitor, inspect, or investigate a Customer for its compliance with this appendix. TCH may appoint agents to carry out its rights under this section.

Schedule 1 – Technical Checklist

Category	Sub-Categories	Complete (yes/no/NA)	Detail or Describe Compensating Controls If "no"	Additional Comments
Oversight	Have the Incident Management, Incident Response, and other appropriate processes been invoked?			
	Has a ticket or tracking mechanism for this cyber threat been created?			
Business Details	Has the impact of the cyber event been identified and communicated to the appropriate business line partners?			
	Has a detailed list been compiled of all detection methods and details communicated appropriately?			
	Have all related or additional attacks been contemplated and excluded? Have any additional attack indicators been detected?			

Indicators	Has a list been compiled including all possibly impacted internal IP addresses?			
	Has a list been compiled with all possible external or remote IP addresses? (including any possibly impacted SaaS or cloud resources)			
	Have all external or remote IP addresses impacted been blocked and/or mitigated?			
Third Party Engagement	Has a complete list of indicators of compromise been compiled?			
	Has the list of indicators been submitted to the required external partners (e.g., FSISAC, ARC)?			
	Has the institution engaged its Managed Security Service Providers (MSSP) as appropriate for intraday or single day event?			
	Has the institution engaged its MSSPs as appropriate for multi-day event?			
Data and Network	Has a list been created with all identified data either modified, corrupted or exfiltrated?			
	For any possibly corrupted data, has it been recovered, reconstructed and/or restored?			
	Were any DNS Issues identified and/or excluded?			

	Were any physical devices impacted? (e.g., servers, routers, load balancers, etc.)			
	Has a list been created of all identified malicious network traffic? If so, has that traffic been sufficiently blocked? If so, have all indicators been updated in appropriate detective controls?			
Vulnerabilities	Have all vulnerabilities been identified? If so, have all the vulnerabilities been patched and/or remediated?			
	Has a validation scan been completed showing that any impacted systems have been mitigated?			
Vector(s)	Has any phishing email(s) identified as part of the cyber-attack? If so, have the links, attachments and/or addresses been blocked? If so, have detective controls been updated to detect additional attempts?			
	Has another vector been identified in the cyberattack?			
	Was this due to a third party or alternative supply-chain component?			
	Is there attribution of the threat actor?			
Access Control	If required, have all passwords been reset, enterprise-wide?			

	If required, have any questionable accounts been disabled?			
	If required, has any unauthorized access been identified? If so, has additional activity been identified?			
	If required, have any impacted service account passwords been reset?			
Types of Attack	Has any Worm, Virus, Ransomware, or any other type of malware been identified?			
	Was a Remote Access Trojan identified?			
	Was a Rootkit installed?			
	Was there any credential dumping and/or acquiring evident in the cyber event?			
	Was there a virus investigation conducted?			
	Were there any external sandbox reports run?			
	Was this a supply chain attack?			

	Was this a potential or confirmed nation-state attack?			
	Is this part of a previously known and documented attack?			
	Was the cyber event a result of anything not contained in other sections of this checklist?			
Insider Threat	Was an Insider Threat User or Group involved in this attack? If so, was it intentional or inadvertent?			
	Was the Insider Threat process invoked and executed as part of the investigation into this attack?			
Controls Modified	Were any new controls added or existing controls enhanced as a result of this attack?			

Schedule 2 – Assurance Requirements

Requirements	Steps to Meet Requirement	Notes/Issues
The institution has completed each of the items in the technical checklist (Schedule 1).	Executive Certification	Communicated to applicable parties
The institution has shared industry-relevant information about the incident through appropriate channels.	The institution has reported indicators and technical details to FSISAC, ARC, and others. The institution has shared with applicable parties any incident details that are unique to CHIPS' operation and relevant to TCH or other Participants' protection of their CHIPS-related systems.	
The institution has received assurance from one or more Managed Security Service Providers that the issue does not exist elsewhere in any of its networks, systems, hardware, software, or locations.	One or more Managed Security Service Providers have performed a check of the institution's systems and advised the institution they do not see evidence of the issue that caused the incident in any of the institution's systems.	Absence of evidence is not evidence of absence but ensuring a third party review of the impacted systems will build confidence that the situation has been remediated appropriately.
The institution has received limited assurance statements from one or more core industry partners (such as, Department of Treasury's OCIP, FBI, Department of Homeland Security, SIFMA, ARC and/ or FS-ISAC) that they do not see any activity or traffic related to the issue that prompted failover.	One or more core industry partners have reviewed the information provided and have advised the institution that they do not see any activity or traffic directed at the institution related to the issue that caused the incident.	Absence of evidence is not evidence of absence, but having industry partners confirm that they also see no evidence of the issue that caused the incident will help ensure that the threat has been extinguished.