




# CFIUS Security Policies

Version 1.00


Date: 15 January 2020

This document contains proprietary information of HCL Technologies Ltd. No part of this document may be reproduced, stored, copied, or transmitted in any form or by means of electronic, mechanical, photocopying or otherwise, without the express consent of HCL Technologies. This document is intended for internal circulation only and not meant for external distribution.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	2 of 93

## Table of Contents:

CFIUS001 - Glossary of Terms Related to CFIUS Security Policies	p. 3
CFIUS010 - CFIUS Governance, Oversight and Notification Policy	p. 10
CFIUS020 - CFIUS Access Control Policy	p. 22
CFIUS030 - CFIUS Product Integrity Policy	p. 34
CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy	p. 47
CFIUS050 - CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment	p. 60
CFIUS060 - CFIUS Physical Security Policy	p. 70
CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers	p. 78
CFIUS080 - CFIUS Background Verification Policy	p. 87
<b>EMPLOYEE ACKNOWLEDGEMENT</b>	<b>p. 93</b>


	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	3 of 93

# CFIUS001

## Glossary of Terms Related to CFIUS Security Policies

Version 1.00

Date: 18 December 2019

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	4 of 93

## 1. Purpose

The purpose of this document is to define the common terms used in the CFIUS Security Policies. Terms used in more than one CFIUS Security Policy will be defined in this Glossary, while terms used in a single CFIUS Security Policy will be defined within that document.

Terms derived directly from definitions in the National Security Agreement made between HCL, International Business Machines (“IBM”), and the U.S. Government are denoted with an asterisk (\*).

## 2. Glossary of Terms

**“Affiliate”** means an entity that controls, is controlled by or shares common control with HCL, where such control arises from either (a) a direct or indirect ownership interest of more than 50% of the outstanding voting stock and/or equivalent interest, or (b) the power to direct or cause the direction of the management and policies, whether through the ownership of voting stock, by contract, or otherwise, equal to that provided by a direct or indirect ownership of more than 50% of the outstanding voting stock and/or equivalent interest.

**“Access Controls”** means processes used to ensure Personnel have no greater information access than is necessary to capably perform their job function.

**“Agreement”** refers to the confidential National Security Agreement made between HCL, International Business Machines (“IBM”), and the U.S. Government, effective June 10, 2019. \*

**“Approved Personnel”** means Personnel approved on the Federal Access Control List to perform a function restricted to U.S. Personnel.

**“Audit”** means the assessment of compliance performed in accordance with the terms of the Agreement, one (1) year after the Effective Date and again every 2 years, unless requested otherwise by CFIUS Monitoring Agencies.


**“Audit Report”** means an assessment of HCL’s compliance with the Agreement developed in accordance with the CFIUS Governance, Notification, and Oversight Policy.\*

**“Authentication”** means a process by which an entity (or a person or computer system) determines whether another entity is who it claims to be.

**“Authorization”** means a process of determining if the end user is permitted to have access to the desired information or system containing the information. Authorization criteria may be based upon a variety of factors such as organizational role, administrative privileges required, applicable law or a combination of factors.

**“Background Verification Council” or “BGV Council”** refers to compliance professionals who review discrepancies or concerns raised by background check results. The BGV Council is made up of HCL’s Global Compliance Lead, the North American Compliance Lead and legal counsel.

**“Committee on Foreign Investment in the United States” or “CFIUS”** means the interagency committee of the United States government authorized to review certain transactions involving foreign investment in the United States (“covered transactions”), in order to determine the effect of such transactions on the national security of the United States pursuant to section 721 of the Defense Production Act of 1950, as amended, or any constituent member thereof acting in such capacity. \*

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	5 of 93

**“CFIUS Governance Committee” or “CGC”** means a committee established by the Board of Director of HCL Technologies, Ltd. for the purpose of periodic internal monitoring of HCL’s compliance with the terms of the Agreement.

**“CFIUS Implementation Leader”** means an HCL Employee appointed to represent an organization involved in the design, development, production and delivery of In-Scope Software Products, or an enabling function, such as Human Resources, to serve as that organization’s focal point for implementing the CFIUS Security Policies.

**“CFIUS Implementation Plan”** means the plan with timelines and milestones for the implementation of the CFIUS Security Policies. \*

**“CFIUS Monitoring Agencies” or “CMAs”** refers to the U.S. Departments of Defense, Justice, and the Treasury. \*

**“CFIUS Security Officer”** means the HCL Security Officer appointed in accordance with the terms of the Agreement. \*

**“CFIUS Security Policies”** means those HCL corporate policies developed and adopted to implement the requirements of the Agreement.

**“CFIUS Security Policies Task Force” or “SPTF”** means a task force that may be established by the CFIUS Governance Committee, from time to time, for purposes of facilitating the establishment, implementation, oversight, and periodic updating of the CFIUS Security Policies, which task force shall be chaired by the CFIUS Security Officer and may include representatives selected by the CFIUS Security Officer, through consultation with the CFIUS Governance Committee, from the teams involved in the design, development, production and delivery of In-Scope Software Products to U.S. Federal Government Customers as well as teams with enabling responsibilities, such as Human Resources.

**“Closing Date”** means June 30, 2019. \*

**“Commercially Reasonable Terms”** means terms consistent with prevailing market and industry standards for like products by a company of similar size and scope taking into account efficacy, safety, and previous contractual commitments. \*

**“Company”** – see definition of “HCL” below.


**“Computer Security Incident Response Team” or “CSIRT”** is the HCL Software cross-functional team that handles a Security Incident tied to data or violation of security policy, led by the Security Implementation Leader with awareness to the CFIUS Security Officer and the HCL corporate information security team.

**“Confidentiality”** the obligation of an individual, organization or business to protect information and not misuse or wrongfully disclose that information.

**“Contractor”** means a business or person that performs a service for HCL under a contract (other than an employment contract with HCL) to which HCL is a party.

**“Cybersecurity Plan”** means the plan governing the protection of the Secure Software Build Environment for the In-Scope Software Products in accordance with the Agreement. \*

**“Employee”** is a person who is on the payrolls of HCL including permanent, fixed term, part time, and expatriate employee subject to the deputation/transfer letter issued, if any.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	6 of 93

“**Encryption**” means the cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used.

“**Federal Access Control List**” means the list maintained by HCL of the U.S. Personnel granted access permissions by HCL (i) to manage the Secure Software Build Environment for the In-Scope Software Products that HCL delivers to U.S. Federal Government Customers, and/or (ii) to provide on-site support at concerned customer locations to U. S. Federal Government Customers, and/or (iii) to perform other job functions restricted to U.S. Personnel. \*

“**Federal Business Partner**” means a third-party entity with which HCL has entered into an exclusive agreement to resell In-Scope Software Products to U.S. Federal Government Customers and provide an infrastructure for doing business with the U.S. Federal Government.

“**Federal Support Center**” or “**FSC**” means a software technical support center located in the continental United States and staffed by Approved Personnel on the Federal Access Control List only.

“**Federal Support Environment**” or “**U.S. Federal Support Environment**” means the ticketing tool and customer data repository dedicated to U.S. Federal Government Customers and accessible only to U.S. Personnel.

“**Former IBM Employee**” or “**Rebadged IBM Employee**” means an employee hired by HCL from IBM because of a partnership, acquisition, or other transaction between the companies.

“**HCL**”, “**Company**”, “**us**”, “**we**” refers to HCL Technologies, Ltd. and HCL America, Inc. \*

“**HCL Software**” is a division of HCL Technologies, Ltd. that operates its primary software business.

“**In-Scope Software Products**” means the HCL software products BigFix, Notes/Domino, Sametime, AppScan, Unica, Digital Experience (Portal), Commerce, and Connections, except products delivered through non-FedRAMP certified SaaS services to U.S. Federal Government Customers. \*

“**Information Security**” means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.


“**International Development Locations Inventory**” means a listing of approved locations outside the United States that HCL utilizes for Source Code development.

“**Known Breach**” means a Suspected Breach that has been investigated by the CFIUS Security Officer and validated as an actual failure of HCL to comply with (i) its obligations specified in the Agreement or (ii) the CFIUS Security Policies.

“**Mobile Device**” means a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.

“**NIST**” means the National Institutes of Standards and Technologies

“**Non-Approved Personnel**” means any Personnel who are not Approved Personnel.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	7 of 93

**“Personnel”** means officers, directors, Employees, Contractors, and individuals otherwise engaged by HCL for professional or technical services who are under the direction and control of HCL and have access to HCL’s information resources.

**“Product Security Incident Response Team”** or **“PSIRT”** consists of a PSIRT program manager and the designated product security incident responders on the product development teams. The program manager is responsible for establishing processes and tools for managing product-related security vulnerabilities and incidents in coordination with product security responders.

**“Product Security Vulnerability”** means an actual Security Vulnerability involving an In-Scope Software Product.

**“Production Build Servers”** means the environments in the United States that transform a selected version of Source Code into a Release of an In-Scope Software Product.

**“Publication Repositories”** means the storage locations housed on publication servers in the United States where Releases of the In-Scope Software Products are available for download by entitled customers.

**“Release”** means a distribution of the In-Scope Software Products which is warranted and made generally available to all entitled customers, including but not limited to major releases (new versions or releases), interim releases (minor releases, modification levels or feature packs), or maintenance releases (fix packs or cumulative refreshes). It does not include temporary and/or non-warranted releases made available to individual customers, including but not limited to Test Fixes or pre-release betas.

**“Secure Engineering Framework Testing Flows”** means the Source Code Scan Release Flow, the Penetration Testing Release Flow, and the Script and Content Publication Flow as defined in the Agreement. \*

**“Secure Software Build Environment”** means the Source Code Repositories, Production Build Servers, and Publication Repositories hosted in the U.S. for the In-Scope Software Products. \*


**“Security Incident”** means a single or series of security events with negative consequences in an information system or network that (i) involve a Product Security Vulnerability, (ii) involve unauthorized access, use, disclosure, disruption, modification, or destruction of HCL’s information systems or information residing therein, (iii) have a significant adverse impact on business operations, or (iv) otherwise violate or present an imminent threat of violation of HCL’s information security policies, acceptable usage policies or standard security practices.

**“Security Vulnerability”** is a weakness which can be exploited by a threat actor, such as an attacker, that increases the likelihood or severity of potential Security Incidents associated with the asset or control.

**“Service Agreement”** means a contract or other agreement that governs the relationship between HCL America Inc. and an approved Third-Party Monitor. \*

**“Source Code”** means the actual, human-intelligible software code that is used to create the application associated with an In-Scope Software Product, and which defines the product’s behavior. \*

**“Source Code Development Process”** means any stage of the design, development, support, or testing and verification of an In-Scope Software Product. Source Code Development Process shall not include activities related to the product that are aesthetic, including but not limited to the industrial design and packaging, or to user documentation (such as product instructions and regulatory compliance information) included with the product. \*

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	8 of 93

"**Source Code Repositories**" means the file storage locations and structures housed on servers in the United States and used to provide version control and access management for the Source Code used to build Releases of the In-Scope Software Products.

"**Support Personnel**" means third-party hardware and software vendors.

"**Suspected Breach**" means a suspected failure of HCL to comply with (i) its obligations specified in the Agreement or (ii) the HCL CFIUS Security Policies that has not been both investigated and validated by the CFIUS Security Officer.

"**Test Fix**" means a temporary non-warranted update made available to an individual customer to correct, debug or validate a correction to a specific problem.

"**Third-Party Auditor**" is a third-party hired to complete an Audit of HCL's compliance with the Agreement. \*

"**Third-Party Entity Service Provider**" means third-parties (other than IBM) engaged by HCL to assist in the Source Code Development Process. \*

"**Third-Party Monitor**" or "**TPM**" is a disinterested third-party who performs verification and compliance monitoring services in connection with the Agreement on an on-going basis in accordance with the Service Agreement. \*

"**Transaction**" means the acquisition of certain assets of IBM, including In-Scope Software Products, by HCL, which was consummated on June 30, 2019. \*

"**U.S. Federal Government Customer Business Identifiable Information**" means the name, address, business telephone number, email address, Internet Protocol address, or any other identifying information of a U.S. Federal Government Customer, to the extent acquired by IBM or HCL through the provision of In-Scope Software Products and related services to such customer, provided U.S. Federal Government Customer Business Identifiable Information does not include de-identified and/or anonymized information that cannot be linked to a particular U.S. Federal Government Customer, and further provided that mere U.S. Federal Government Customer agency, department or entity names, references or acronyms alone without any further customer identifying information are not considered U.S. Federal Government Customer Business Identifiable Information if said information relates to unclassified work that is otherwise discoverable in the public domain. \*


"**U.S. Federal Government Customer Support Records**" means support records (including vulnerability data) of a U.S. Federal Government Customer obtained by IBM or HCL through the provision of In-Scope Software Products support services to such customer, which for example may be contained in support tickets, log files or other information recorded for debugging purposes, provided U.S. Federal Government Customer Support Records does not include de-identified and/or anonymized information that cannot be linked to a particular U.S. Federal Government Customer. \*

"**U.S. Federal Government Customers**" refers to the Federal departments, agencies, and other entities—including, but not limited to the CFIUS Monitoring Agencies—and the acquisition or information technology professionals, contractors and agents thereof, to the extent they (i) have a direct or indirect contract with HCL America to utilize, or (ii) have been identified in advance to the HCL Security Officer by Federal departments, agencies, and other entities including, but not limited to, the CFIUS Monitoring Agencies as utilizing, the In-Scope Software Products on information systems and networks maintained by their respective agencies; provided such term does not refer to any entity or person (x) receiving products or services from HCL through non-FedRAMP certified SaaS services or support, or (y) in their capacity as a recipient of products that are not In-Scope Software Products or related services. \*

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	9 of 93

“U.S. Federal Government Customer Data” includes both U.S. Federal Government Customer Business Identifiable Information and U.S. Federal Government Customer Support Records.

“U.S. Personnel” means Personnel who are United States citizens and located in the United States. \*


### 3. Related Documents

The following CFIUS Security Policies are associated with this glossary:

1. CFIUS010 - CFIUS Governance, Oversight, and Notification Policy
2. CFIUS020 – CFIUS Access Control Policy
3. CFIUS030 - CFIUS Product Integrity Policy
4. CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy
5. CFIUS050 - CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment
6. CFIUS060 - CFIUS Physical Security Policy
7. CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers
8. CFIUS080 - CFIUS Background Verification Policy
9. Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products

### 4. Change Log

Version	Date	Author(s)	Summary of Changes
1.00	December 18, 2019	Karen Plonty	Final document
1.00	January 15, 2020	Karen Plonty	Approved by CFIUS Governance Committee without change.


	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	10 of 93

# CFIUS010

## CFIUS Governance, Oversight, and Notification Policy

Version 1.00

Date: 18 December 2019

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	11 of 93

## 1. Purpose

The purpose of this CFIUS Governance, Oversight and Notification Policy (this “Policy”) is to implement the requirements of the National Security Agreement made among HCL, International Business Machines (“IBM”), and the U.S. Government.

This Policy creates the framework for implementation of the Agreement, through the various security policies listed in Section 6.1 (the “CFIUS Security Policies”), which augment the HCL information security policies and procedures with specific additional policies and procedures necessary to implement the requirements of the Agreement.

In addition, the CFIUS Security Policies implement the direction from the HCL Technologies Ltd. Board of Directors to at all times maintain policies and practices that ensure the safeguarding of information and the performing of contracts and programs for the U.S. Government in accordance with the National Security Agreement.

## 2. Scope

The CFIUS Security Policies apply to all HCL Personnel, to the extent applicable based on their job function. The policies and procedures for breach reporting in Section 6.6 of this Policy apply to all HCL Personnel regardless of job function.

All CFIUS Security Policies described in Section 6.1 of this Policy apply to all HCL Personnel engaged in activities involving the Source Code Development Process for In-Scope Software Products, the Secure Software Build Environment, U.S. Federal Government Customer Data, or other information regarding the performance of contracts and programs for the U.S. Federal Government.

## 3. Definitions

Capitalized terms used herein and not otherwise defined have the meaning set forth in the Glossary (CFIUS001 - Glossary of Terms Related to CFIUS Security Policies).

## 4. Policy Statements

It is the policy of HCL that:

All HCL Personnel must comply with the CFIUS Security Policies, to the extent applicable.

HCL will cooperate fully with the CFIUS Monitoring Agencies’ in their efforts to monitor HCL’s compliance with the Agreement, including providing access to HCL facilities as described in Section 6.5 of this Policy and meeting with the CFIUS Monitoring Agencies as required by the Agreement and more fully described in Section 6.10 of this Policy.

HCL Personnel must promptly report any Suspected Breach of the CFIUS Security Policies as described in Section 6.6 of this Policy and must cooperate fully with the investigation of any Suspected Breach.

HCL may not take retaliatory action against any HCL Personnel who in good faith reports a Suspected Breach.

Classification – Internal

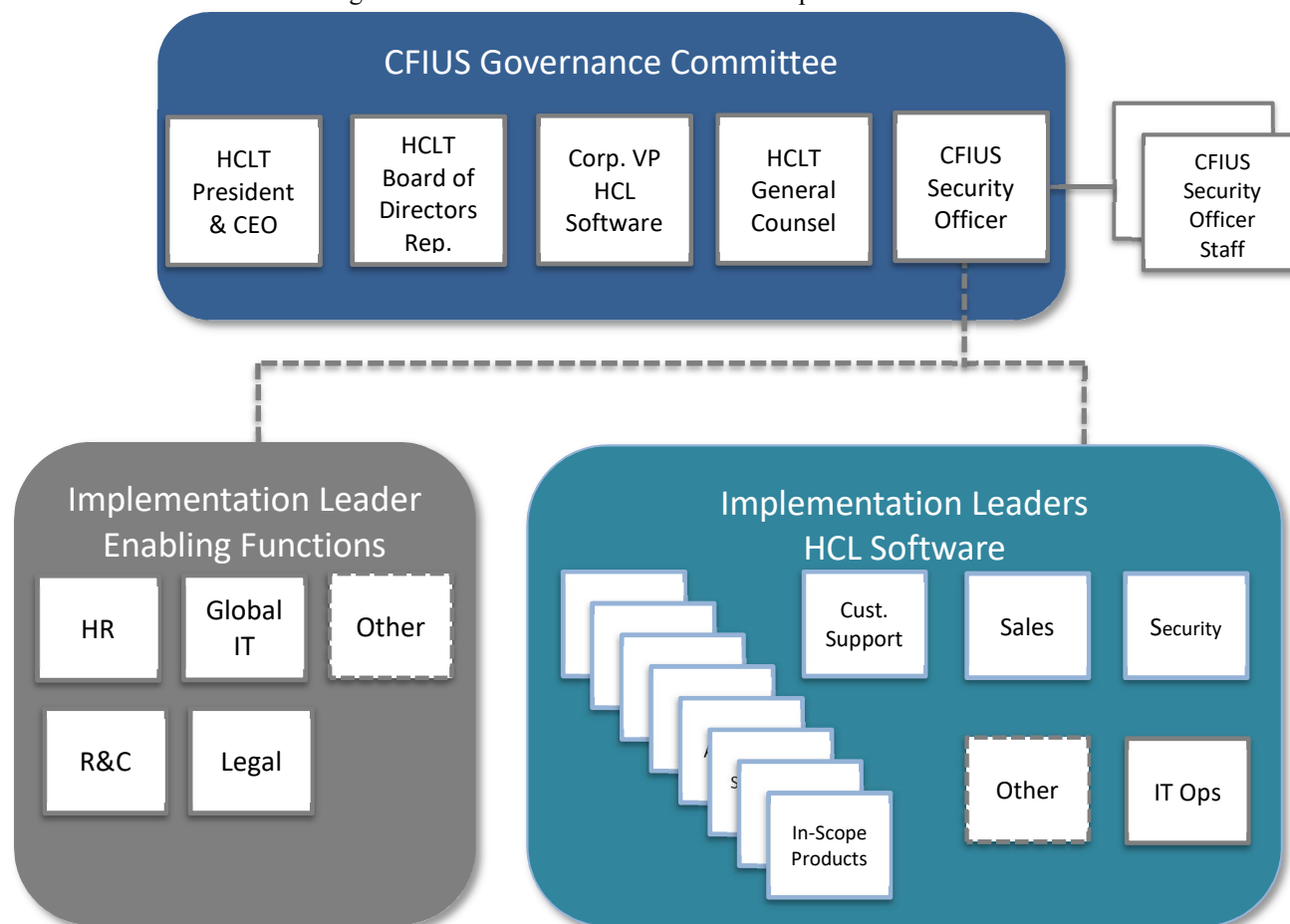
Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

<b>HCL</b>	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	12 of 93

## 5. Roles and Responsibilities

Figure 1 depicts the roles and responsibilities for HCL CFIUS governance described in this section.

Figure 1: CFIUS Governance Roles and Responsibilities



### 5.1 CFIUS Governance Committee

#### *Committee Description*


The HCL Technologies Ltd. Board of Directors has established at its sole discretion a CFIUS Governance Committee (“CGC”) to monitor and oversee compliance with the Company’s obligations toward CFIUS. The CGC shall meet on a schedule that it establishes.

The CGC shall be made up of:

- President & CEO of HCL Technologies Ltd.
- A representative of the HCL Technologies Ltd. Board of Directors
- Corporate Vice President – HCL Software
- General Counsel of HCL Technologies Ltd.
- The CFIUS Security Officer

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	13 of 93

As necessary, the members of the CGC, except for the CFIUS Security Officer, may be rotated or replaced to better assist with the Company's compliance efforts.

### *Committee Responsibilities*

The CGC when constituted shall, subject to delegation by the HCL Technologies Ltd. board, have the authority to:

Concerns raised regarding the Non-Retaliation Policy: Oversee the investigation of any reports of violations of the non-retaliation policy, make the final determination, and take appropriate disciplinary action, as necessary.

Escalations from the CFIUS Security Officer: Review any matter which the CFIUS Security Officer may escalate for their attention regarding HCL's compliance with the Company's obligations toward CFIUS.

Appointing or replacing the CFIUS Security Officer: Appoint and maintain a qualified CFIUS Security Officer who will oversee and administer HCL's compliance with its obligations toward CFIUS. (For purposes of appointing or replacing the CFIUS Security Officer, any current CFIUS Security Officer will be recused from such action.)

- HCL must notify the CFIUS Monitoring Agencies of any proposed change to the CFIUS Security Officer at least fifteen (15) business days in advance of such change, unless the CFIUS Security Officer resigns, becomes incapacitated, or HCL removes the CFIUS Security Officer for cause or in connection with the performance of the CFIUS Security Officer's duties of another position contemporaneously held by the CFIUS Security Officer, in which case HCL must immediately provide the CFIUS Monitoring Agencies with notification of, and the basis for, the removal.
- The replacement of the CFIUS Security Officer will be subject to the CFIUS Monitoring Agencies' review and non-objection and may be subject to a background check at the CFIUS Monitoring Agencies' sole discretion.
- If the CFIUS Monitoring Agencies do not object to, or do not require a background check of, the CFIUS Security Officer nominee within fifteen (15) business days of receiving notice of the nominee, the lack of action will constitute non-objection to the nominee.
- If the CFIUS Monitoring Agencies object to a nominee, HCL must nominate an alternative within fifteen (15) business days of the objection.

Monitoring the Status of HCL's Obligations Toward CFIUS: Monitor the status of HCL's obligations toward CFIUS on behalf of the HCL Technologies Ltd. Board of Directors through regular reports from the CFIUS Security Officer as necessary.

Authorizing the CFIUS Security Officer: Ensure that the CFIUS Security Officer has the appropriate senior-level authority and resources to perform his or her duties. The CGC must further ensure that the CFIUS Security Officer has access to all appropriate business records to perform his or her duties.

Approval of Third-Party Oversight: Review and approve the selection of the CFIUS Third-Party Monitor as outlined in Section 6.3 of this Policy and the CFIUS Third-Party Auditor as outlined in Section 6.4 of this Policy.

Approval of CFIUS Security Policies: Review and approve the CFIUS Security Policies and any subsequent material changes as outlined in Section 6.1 of this Policy.


## **5.2 CFIUS Security Officer**

The CFIUS Security Officer:

- Is responsible for ensuring HCL's compliance with the Agreement.

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	14 of 93

- Is responsible for development, administration, maintenance, and implementation of the CFIUS Security Policies as described in Section 6.1 of this Policy.
- Approves any exceptions to the CFIUS Security Policies.
- May, from time to time, apply the requirements of any CFIUS Security Policy to products (or components thereof) that are not In-Scope Software Products, to the extent the CFIUS Security Officer deems such application reasonably necessary to ensure HCL's compliance with the Agreement
- Is responsible for overseeing appropriate periodic training of HCL officers, directors, and Personnel who perform services relating to In-Scope Software Products delivered to U.S. Federal Government Customers regarding compliance with the Security Policies.
- Selects and recommends a CFIUS Third-Party Monitor and a CFIUS Third-Party Auditor for the CGC's review and approval.
- Record-keeping in accordance with this Policy.
- Investigates all reported Suspected Breaches.
- Reports any Known Breaches in accordance with the CFIUS Security Policies.
- Approves the appointment of the CFIUS Implementation Leaders

### 5.3 CFIUS Implementation Leaders

The CFIUS Security Officer may, at his or her discretion, approve HCL Employees<sup>1</sup> appointed to represent organizations involved in the production and delivery of In-Scope Software Products, or enabling functions, such as Human Resources, to serve as Implementation Leaders for the CFIUS Security Policies and the CFIUS Implementation Plan. The Implementation Leaders must assist the CFIUS Security Officer with implementation and oversight of the CFIUS Security Policies for their respective organizations.

The CFIUS Implementation Leaders:

- Ensure compliance with the CFIUS Security Policies in their area of responsibility
- Lead the development of appropriate CFIUS Security Policies
- Have primary responsibility for implementation of CFIUS policies and procedures
- Integrate CFIUS compliance into business operations
- Support development and deployment of training
- Support periodic communication of CFIUS obligations to their organization
- Participate in the CFIUS Security Policy Task Force ("SPTF")
- Assist with record-keeping in accordance with this Policy as directed by the CFIUS Security Officer
- Provide business records upon request by the CFIUS Security Officer, Third-Party Monitor and/or Third-Party Auditor
- Serve as primary contact for reports of Suspected Breaches in their organization
- Support CFIUS Suspected Breach investigations
- Support Third-Party Audits


## 6. Policy Details and Corresponding Procedures

### 6.1 CFIUS Security Policies

#### *Relationship to HCL Information Security Policies*

HCL must adopt and maintain the CFIUS Security Policies to facilitate HCL's compliance with its obligations under the Agreement. The CFIUS Security Officer will be the cognizant authority for the CFIUS Security Policies, subject to the oversight of the CGC, as necessary. The CFIUS Security Policies are the following:

<sup>1</sup> CFIUS Implementation Leaders may not be Contractors or third-parties.

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	15 of 93

- CFIUS001 - Glossary of Terms Related to CFIUS Security Policies
- CFIUS010 - CFIUS Governance, Oversight, and Notification Policy (i.e. this Policy)
- CFIUS020 - CFIUS Access Control Policy
- CFIUS030 - CFIUS Product Integrity Policy
- CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy
- CFIUS050 - CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment
- CFIUS060 - CFIUS Physical Security Policy
- CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers
- CFIUS080 - CFIUS Background Verification Policy

The CFIUS Security Policies augment ISMA012 – Information Security Policy and other HCL information security policies and procedures with specific additional policies and procedures necessary to implement the requirements of the Agreement. In case of any conflict, the applicable CFIUS Security Policies supersede ISMA012 – Information Security Policy and other HCL information security policies and procedures.

### *Updates to the CFIUS Security Policies*

The Security Policy Task Force (“SPTF”) will consist of the CFIUS Security Officer and Implementation Leaders and may, from time to time, update the CFIUS Security Policies. The CFIUS Security Policies must be reviewed by the SPTF once per year at minimum, to determine whether any updates are necessary. Subject to compliance with HCL’s policy adoption procedures, the SPTF must submit any material change to the CFIUS Security Policies to the CFIUS Governance Committee for approval; and following such approval but at least 10 business days prior to adoption, the SPTF shall submit such change to the CFIUS Monitoring Agencies, for non-objection. If the CFIUS Monitoring Agencies do not object to such change, then non-objection shall be presumed and the change may be implemented; provided that to prevent the actual or possible violation of any statute or regulation, or actual or possible damage to HCL or under other exigent circumstances, such change may be implemented without prior notice to the CFIUS Monitoring Agencies, provided further that the CFIUS Monitoring Agencies shall be notified in writing concurrently with such implementation.

HCL must maintain a library of the written CFIUS Security Policies accessible to the HCL Personnel who are in scope for each respective CFIUS Security Policy.

## **6.2 Training**


The CFIUS Security Officer is responsible for overseeing appropriate periodic training of HCL officers, directors, and Personnel who perform services relating to In-Scope Software Products delivered to U.S. Federal Government Customers. Training will be commensurate to the job functions and duties of each group.

HCL Personnel must complete all applicable required training within the specified deadlines.

All HCL reporting managers must ensure that all Personnel that they manage complete the applicable required training within the specified deadlines.

## **6.3 Third-Party Monitor**

HCL must contract with and pay for a disinterested third-party approved by the CFIUS Monitoring Agencies to serve as a Third-Party Monitor (“TPM”) for the purposes of performing verification and compliance monitoring services in connection with HCL’s obligations toward CFIUS. HCL must ensure that the Third-Party Monitor is an entity organized under the laws of the United States or of any state, territory, possession or district of the United

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	16 of 93

States. HCL must provide to the CFIUS Monitoring Agencies, upon request, a copy of their service agreement with the Third-Party Monitor, which shall include terms and conditions consistent with the Agreement.

### *Third-Party Monitor Accesses*

HCL must grant the TPM, upon reasonable prior notice and during normal business hours, access to all HCL facilities, systems, networks, personnel, and information necessary to perform its responsibilities. Further, HCL must grant the TPM access to the Product Security Incident Response Team (PSIRT) portal and processes where consumers, researchers, reporters, or other third parties can report a potential security vulnerability or concern with one of the In-Scope Software Products.

### *Non-Retaliation Against the Third-Party Monitor*

HCL may not take retaliatory action against the TPM including, but not limited to, withholding payment due to the TPM, for reasonable actions taken by the TPM to fulfill its responsibilities under the Agreement, as detailed in the service agreement between HCL and the TPM and as determined by the CFIUS Monitoring Agencies in their reasonable discretion.

## **6.4 Third-Party Auditor**

HCL must retain and pay for a Third-Party Auditor approved by the CFIUS Monitoring Agencies to complete an assessment of compliance with its HCL's obligations toward CFIUS and to provide an Audit Report to the CFIUS Monitoring Agencies. HCL must provide to the CFIUS Monitoring Agencies, upon request, a copy of their Service Agreement with the Third-Party Auditor, which shall include terms and conditions consistent with the Agreement.

### *Procedures for Developing the Audit Scope and Methodology*

HCL must submit the scope and methodology for the Audit for approval by the CFIUS Monitoring Agencies. HCL must submit the scope and methodology of the first such Audit no later than one (1) year following the Closing Date. HCL must address any objections to the proposed Audit scope and methodology from the CFIUS Monitoring Agencies to the CFIUS Monitoring Agencies' reasonable satisfaction within twenty (20) business days of the date of the objection. If the CFIUS Monitoring Agencies do not provide written non-objection to the proposed Audit scope and methodology within ten (10) business days of notice, HCL will deem the proposal approved.

### *Subsequent Audits*


HCL must retain a Third-Party Auditor to conduct subsequent Audits every other year following the first Audit Report unless the CFIUS Monitoring Agencies request subsequent Audits more frequently; provided that the CFIUS Monitoring Agencies may not require an Audit more than three (3) times within any five (5) consecutive years.

## **6.5 Access and Inspection**

HCL must accommodate requests from the CFIUS Monitoring Agencies to inspect any HCL facility involved in the development, maintenance, marketing, or sale of the In-Scope Software Products during normal business hours, provided such request has been made with three (3) business days' advance written notice of the requested date; provided that, in exigent circumstances, HCL must accommodate requests for inspection from the CFIUS Monitoring Agencies with no advance notice.

During such inspections, HCL must facilitate CFIUS Monitoring Agencies' access to Personnel, books and records, equipment, servers, and facilities and premises of HCL, as well as information concerning logical, technical,



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	17 of 93

physical, or management measures that are the subject of the Agreement for purposes of confirming compliance therewith.

HCL will permit and facilitate CFIUS Monitoring Agencies' access to HCL systems and networks involved with the Secure Software Build Environment for purposes of assessing HCL's compliance with the Cybersecurity Plan upon reasonable prior notice and during normal business hours.

Any HCL Personnel who receives a request for an inspection or for access from the CFIUS Monitoring Agencies, regardless of whether the CFIUS Monitoring Agencies have provided advance notice, must notify the CFIUS Security Officer immediately.

## 6.6 Reporting and Notification

### *Reporting Suspected Breaches and Known Breaches*

All HCL Personnel must promptly report any Suspected Breach to the CFIUS Implementation Leader assigned to their organization or function. Personnel are required to report any Suspected Breaches of CFIUS Security Policies, including but not limited to:

- Any suspected unauthorized access to the Secure Software Build Environment or Federal Support Environment
- Any suspected unauthorized access to or disclosure of U.S. Federal Government Customer Data
- Any suspected compromise or unauthorized change to HCL product code regardless of whether the code was introduced into the Secure Software Build Environment or not
- Any suspected Source Code development performed from a location outside the U.S. not on the International Development Locations Inventory (see Section 6.7)


The receiving CFIUS Implementation Leader shall conduct a preliminary investigation to determine whether reported Suspected Breach may constitute a breach. If the receiving CFIUS Implementation Leader's preliminary investigation determines that the reported Suspected Breach clearly does not constitute a breach, he or she may independently take appropriate corrective action based on the results of the preliminary investigation. If the receiving CFIUS Implementation Leader's preliminary investigation determines that the reported Suspected Breach may constitute a breach or requires further review, he or she shall promptly forward the Suspected Breach report and results of the preliminary investigation to the CFIUS Security Officer. The CFIUS Implementation Leader also shall notify the CFIUS Security Officer of any and all reported Suspected Breaches that such Implementation Leader determines after preliminary investigation do not constitute a breach.

Upon receipt of a Suspected Breach report from the CFIUS Implementation Leader, the CFIUS Security Officer shall promptly open an investigation of the Suspected Breach to determine if the reported Suspected Breach constitutes a breach and notify the TPM. Subject to the immediately following paragraph, upon determining that any Suspected Breach constitutes a breach, such breach shall be deemed a Known Breach and the CFIUS Security Officer shall promptly notify the CFIUS Monitoring Agencies and the TPM. At his or her discretion, the CFIUS Security Officer may include information indicating whether such Known Breach is technical or material in nature.

If the CFIUS Security Officer cannot, within five (5) business days of opening an investigation, reach a determination as to whether a reported Suspected Breach constitutes a breach, the CFIUS Security Officer shall notify the CFIUS Monitoring Agencies of the reported Suspected Breach and provide an estimate as to when his or her investigation of such Suspect Breach will conclude.

### *Suspected Breaches and Known Breaches Involving U.S. Federal Government Customer Data*

If CFIUS Security Officer determines the reported Suspected Breach involves a breach or unauthorized disclosure of U.S. Federal Government Customer Data in violation of the CFIUS Security Policies, such breach shall be deemed a

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	18 of 93

Known Breach and, subject to the following paragraph, the CFIUS Security Officer must notify the CFIUS Monitoring Agencies and the TPM of the Known Breach within (24) hours of making such determination.

During the investigation of a Suspected Breach, the CFIUS Security Officer, in consultation with the TPM, may determine that the Suspected Breach involves isolated instances of non-sensitive U.S. Federal Government Customer Business Identifiable Information, e.g. individual U.S. Federal Government Customer names and/or email addresses. The CFIUS Security Officer shall notify the CFIUS Monitoring Agencies every quarter of all Known Breaches involving such isolated instances of non-sensitive U.S. Federal Government Customer Business Identifiable Information in the quarterly notification period.

### *Reporting Contact Initiated by U.S. Federal Government Customers to Non-Approved Personnel*

All HCL Personnel must promptly report any contact initiated by a U.S. Federal Government Customer to Non-Approved Personnel to the CFIUS Implementation Leader assigned to their organization or function. The CFIUS Implementation Leader shall re-direct the U.S. Federal Government Customer to the designated channels and procedures HCL has established for communication with U.S. Federal Government Customers in CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy, and must promptly notify the CFIUS Security Officer. The CFIUS Security Officer shall promptly report such contacts to the TPM and shall notify the CFIUS Monitoring Agencies of all such contacts every quarter.

If a U.S. Federal Government Customer elects to contact Non-Approved Personnel, through other than the designated channels and procedures established by HCL in CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy, the resultant communication shall not alone constitute a breach of this Policy by HCL.

### *Notifications Regarding Unauthorized Code Changes*


HCL shall notify the CFIUS Monitoring Agencies and the TPM of any discovered compromise or unauthorized change to HCL product code for the In-Scope Software Products regardless of whether the code was introduced into the Secure Software Build Environment or not, pursuant to the procedure in this Policy for notification of Known Breaches.

## **6.7 Development Locations Outside the U.S.**

HCL shall maintain an International Development Locations Inventory of locations outside the United States that the Company utilizes for Source Code development for the In-Scope Software Products (see CFIUS030 - CFIUS Product Integrity Policy). No person working outside the United States is permitted to conduct Source Code development unless that person's work location is listed on the International Development Locations Inventory.

HCL shall notify the CFIUS Monitoring Agencies of any planned additional international development locations at least sixty (60) calendar days in advance, including a statement of the rationale for the additional location or locations in its notification. If the CFIUS Monitoring Agencies do not provide written objection within fifteen (15) business days of receipt of such notice, the additional location or locations will be deemed approved pursuant to the Agreement. If the CFIUS Monitoring Agencies object within such 15-day period, HCL may not add the location to the International Development Locations Inventory without subsequent written approval by the CFIUS Monitoring Agencies.

Whenever an HCL reporting manager wishes to modify the job function of any existing Personnel working outside the United States such that the Personnel's new job function includes Source Code development, that HCL reporting manager must first consult the International Development Locations Inventory. If the Personnel's job location is not listed in the International Development Locations Inventory, the Personnel's job function must not change to include

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	19 of 93

Source Code development. HCL reporting managers may submit requests for additions to the International Development Locations Inventory to the CFIUS Security Officer.

Whenever a prospective Personnel located outside the United States is a candidate to be engaged for a job function that includes Source Code development, the Human Resources Implementation Leader or his/her delegate overseeing the prospective Personnel's engagement must consult the International Development Locations Inventory. If the prospective Personnel's location is not on the International Development Locations Inventory, the Human Resources Implementation Leader must not approve the prospective Personnel's engagement for Source Code development. The Human Resources Implementation Leader may submit requests for additions to the International Development Locations Inventory to the CFIUS Security Officer.

## 6.8 Third-Party Entity Service Providers

HCL shall maintain a Third-Party Entity Service Provider Inventory of the approved Third-Party Entity Service Providers who are engaged by HCL to assist in the Source Code Development Process (see CFIUS030 - CFIUS Product Integrity Policy). Third-party entities may not be engaged by HCL to assist with the Source Code Development Process unless they are listed on the Third-Party Entity Service Provider Inventory.

Whenever HCL intends to add a Third-Party Entity Service Provider to the Third-Party Entity Service Provider Inventory, HCL must notify the CFIUS Monitoring Agencies of the proposed change in advance. If the CFIUS Monitoring Agencies do not provide written objection within fifteen (15) business days of notice, the proposal will be deemed approved. If the CFIUS Monitoring Agencies object, HCL may not add the third-party entity to the Third-Party Service Provider Inventory.

Before HCL enters into an agreement with any new Third-Party Entity Service Provider to assist with the Source Code Development Process for the In-Scope Software products, the Implementation Leader must first consult the Third-Party Entity Service Provider Inventory. If the Third-Party Entity Service Provider is not listed in the Third-Party Entity Service Provider Inventory, the Implementation Leader must not enter into the agreement. The Implementation Leader may submit requests for additions to the Third-Party Entity Service Provider Inventory to the CFIUS Security Officer.

## 6.9 Supply of the In-Scope Software Products

Subject to the notice requirement stated below, HCL will continue development, security maintenance, and source code updates at the product level for the In-Scope Software Products and will provide the In-Scope Software Products to U.S. Federal Government Customers upon Commercially Reasonable Terms.

Should HCL intend to cease development, security maintenance, or other technical support (including Source Code updates) for any In-Scope Software Products, HCL must provide written notice to the CFIUS Monitoring Agencies at least two (2) years prior to such cessation. HCL may decide to discontinue support for specifically designated releases or versions of the In-Scope Software Products without notification to the CFIUS Monitoring Agencies.

## 6.10 Information Meetings


At the request of the CFIUS Monitoring Agencies, HCL must meet with the CFIUS Monitoring Agencies not less than once every twelve (12) months, at a mutually agreed upon time and location (or by telephone).

The agenda for such meetings or teleconferences will include the following:

- compliance with the Agreement;

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	20 of 93

- any ongoing business operations affecting the delivery of the In-Scope Software Products to U.S. Federal Government Customers;
- any changes in the technology, market or economic environment that may affect the supply of the In-Scope Software Products to U.S. Federal Government Customers; and
- any planned action by HCL or its affiliates that may affect the supply or integrity of the In-Scope Software Products.

## 6.11 Consequences for Violation

HCL expects all Personnel to comply with the CFIUS Security Policies. If a question arises regarding compliance with the CFIUS Security Policies, Personnel are expected to contact their Implementation Leader or email CFIUS@hcl.com. The Implementation Leader or HCL Security Officer will analyze any query and respond to such Personnel with guidance.

Failure on the part of Personnel to follow the CFIUS Security Policies could result in possible disciplinary action against responsible Personnel up to and including the individual's termination.

## 7. Audit & Record-Keeping

HCL must maintain certain records of its activities executing the policies and procedures in this document for purposes of supporting future audits of its compliance with its obligations toward CFIUS.

### 7.1 Retention Policy

HCL must retain the records identified in this section for a minimum of three years. For these records, this retention period supersedes any applicable shorter retention period established in the HCL Records Retention and Destruction Policy. To the extent that the HCL Records Retention and Destruction Policy schedules require a longer period for these records, the HCL Records Retention and Destruction Policy applies.

### 7.2 Training Records

HCL must retain records of training completion for all Personnel who must receive CFIUS compliance training pursuant to this policy. HCL will audit these records annually to confirm that Personnel have received training appropriate to their job function.

### 7.3 CFIUS Notification Records

HCL must retain records of all notifications made to the CFIUS Monitoring Agencies in accordance with the Agreement.

### 7.4 International Development Locations Inventory Change Log


HCL will maintain a change log recording approved updates to the International Development Locations Inventory (see CFIUS030 - CFIUS Product Integrity Policy).

### 7.5 Third-Party Entity Service Provider Inventory Change Log

HCL will maintain a change log recording approved updates to the Third-Party Entity Service Provider Inventory.

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	21 of 93

## 7.6 CFIUS Security Policy Change Control Records

HCL will maintain a change log recording approved updates to the CFIUS Security Policies.


## 8. Related Documents

The following related documents are associated with this policy:

10. ISMA012 – Information Security Policy
11. [HCL Records Retention and Destruction Policy](#)
12. CFIUS001 - Glossary of Terms Related to CFIUS Security Policies
13. CFIUS020 – CFIUS Access Control Policy
14. CFIUS030 - CFIUS Product Integrity Policy
15. CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy
16. CFIUS050 - CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment
17. CFIUS060 - CFIUS Physical Security Policy
18. CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers
19. CFIUS080 - CFIUS Background Verification Policy
20. Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products

## 9. Change Log

Version	Date	Author(s)	Summary of Changes
1.00	December 18, 2019	Karen Plonty	Final document
1.00	January 15, 2020	Karen Plonty	Approved by CFIUS Governance Committee without change.


	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	22 of 93

# CFIUS020

## CFIUS Access Control Policy

Version 1.00

Date: 18 December 2019

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	23 of 93

## 1. Purpose

The purpose of this document is to implement the requirements for establishing Federal Access Control List protocols for U.S. Personnel in accordance with the National Security Agreement made among HCL, International Business Machines (“IBM”), and the U.S. Government.

## 2. Scope

This document covers the policies and procedures for establishing and using the Federal Access Control List (“FACL”) to control physical and logical access to all facilities, systems, databases, applications, information, and job functions that are restricted to U.S. Personnel by the National Security Agreement.

The requirements in this document apply to all HCL Personnel company-wide involved in:

- the Source Code Development Process for the In-Scope Software Products,
- managing the Secure Software Build Environment,
- overseeing the Secure Engineering Framework Testing Flows for the In-Scope Software Products,
- supporting In-Scope Software Products delivered to U.S. Federal Government Customers,
- accessing U.S. Federal Government Customer Support Records, or
- accessing U.S. Federal Government Customer Business Identifiable Information.

## 3. Definitions

Capitalized terms used herein and not otherwise defined have the meaning set forth in the Glossary (CFIUS001 – Glossary of Terms Related to CFIUS Security Policies).

## 4. Policy Statements

### 4.1 Use of Federal Access Control List for Access Control and Authorization


Management of an individual’s access to, and authorizations for, facilities, servers, systems and applications comprising the Secure Software Build Environment and the Federal Support Environment must be determined and validated by querying a person’s status on the Federal Access Control List.

HCL servers, systems and applications must implement electronic protections or other mechanisms so that only Approved Personnel are granted logical access with appropriate authorizations to servers, systems and applications comprising the Secure Software Build Environment and the Federal Support Environment.

An Information Protection Plan must be developed, documented and implemented for each server, system and application comprising the Secure Software Build Environment and the Federal Support Environment, describing in detail how access will be controlled to comply with this Policy (see Section 6.7).

HCL facilities shall implement physical access controls so that only Approved Personnel have physical access to servers and systems comprising the Secure Software Build Environment and the Federal Support Environment as described in CFIUS060 - CFIUS Physical Security Policy.



	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	24 of 93

Periodic audits must be performed to verify that only Approved Personnel are on the access control lists with appropriate authorizations for facilities, servers, systems and applications comprising the Secure Software Build Environment and the Federal Support Environment.

Physical and logical access to facilities, systems and applications comprising the Secure Software Build Environment and the Federal Support Environment shall be logged. The HCL CFIUS Security Officer and the Third-Party Monitor must have access to all logs.

Personnel shall be promptly removed from the Federal Access Control List when they no longer have a business need for access, when they no longer meet the requirements as determined by the CFIUS Security Officer, or when they cease to be employed or otherwise engaged by HCL or a U.S. subsidiary of HCL for professional or technical services.

## 4.2 Secure Software Build Environment

### 4.2.1 Access by Approved Personnel

Except for access rights for HCL Non-Approved Personnel described in Section 4.2.3, only Approved Personnel or individuals who are IBM employees may access the Secure Software Build Environment as described in CFIUS030 - CFIUS Product Integrity Policy.

Only Approved Personnel shall have server-level access privileges to the servers housing the Source Code Repositories. Source Code Repositories shall be managed solely by Approved Personnel as described in CFIUS030 - CFIUS Product Integrity Policy.

Only Approved Personnel shall select the Source Code for a Release of an In-Scope Software Product and initiate a production build. Only Approved Personnel shall be able to make modifications to the selected Source Code once Approved Personnel have selected the Source Code for a Release of an In-Scope Software Product and initiated a production build as described in CFIUS030 - CFIUS Product Integrity Policy.

Production Build Servers and build automation servers and tools must be managed by Approved Personnel as described in CFIUS030 - CFIUS Product Integrity Policy.

Publication Repositories for U.S. Federal Government Customers must be managed by Approved Personnel as described in CFIUS030 - CFIUS Product Integrity Policy.


### 4.2.2 Access by IBM Employees

Individuals who are IBM employees may have the same access rights to the Secure Software Build Environment as Approved Personnel. Access to the Secure Software Build Environment by IBM employees requires such employees to be onboarded as HCL Contractors, complete HCL mandatory compliance training, and be approved by the CFIUS Security Officer.

### 4.2.3 Access by Non-Approved Personnel

Source Code may be submitted to the Source Code Repositories only by Approved Personnel or by Non-Approved Personnel permanently based in and working from locations on the International Development Locations Inventory (see CFIUS030 - CFIUS Product Integrity Policy).



	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	25 of 93

Access to the Source Code Repositories by Non-Approved Personnel shall be limited to read-write access and/or read-only access to only the Source Code necessary for their respective scope of work and role.

Access to the executable code and object code artifacts from Production Build Servers by Non-Approved Personnel shall be limited to read-only access privileges for the components required for further Source Code development within their respective scope of work and role (see CFIUS030 - CFIUS Product Integrity Policy).

After the build process is initiated by Approved Personnel, Non-Approved Personnel may initiate test jobs to test any Release, or any Test Fixes for U.S. Federal Government customers, and may monitor test results.

For the avoidance of doubt, Non-Approved Personnel shall not have access privileges to:

- select the Source Code for a Release of an In-Scope Software Product,
- make modifications to the selected Source Code once Approved Personnel have selected the Source Code for a Release of an In-Scope Software Product,
- initiate the build process for any Release of an In-Scope Software Product or for any Test Fix delivered to U.S. Federal Government Customers, or
- transfer the Release to Publication Repositories for U.S. Federal Government Customers.

### 4.3 Secure Engineering Framework Testing Flows

For In-Scope Software Products, HCL must adhere to the Secure Engineering Framework Testing Flows under the supervision of Approved Personnel as defined in CFIUS030 - CFIUS Product Integrity Policy. Approved Personnel shall perform the following functions:

- Validation and verification of source code scanning and results of the scan for releases with compiled object code, to ensure that high severity issues are resolved, confirmed as not applicable, or have an approved mitigation plan prior to publication of the Release
- Visual review and inspection of scripts and content for scripting and content releases where automated tools are not available
- Annual product penetration testing

### 4.4 U.S. Federal Government Customer Data

Access to U.S. Federal Government Customer Business Identifiable Information and U.S. Federal Government Customer Support Records shall be restricted to Approved Personnel (see CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy).

U.S. Federal Government Customer Data may only be stored in servers, systems and applications approved by the CFIUS Security Officer. Access to such servers, systems and applications must be restricted to Approved Personnel.

### 4.5 Federal Support Environment


HCL must ensure that U.S. Federal Government Customer support requests are received by only Approved Personnel. U.S. Federal Government Customer support requests shall be handled within a ticketing tool dedicated to U.S. Federal Government Customers and accessible only to Approved Personnel (see CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy).

Only Approved Personnel shall have access to servers, systems, and applications comprising the Federal Support Environment, including the ticketing tool and customer data repository dedicated to U.S. Federal Government Customers.

### 4.6 On-Site Support at U.S. Federal Government Customer Locations

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	26 of 93

Any time a U.S. Federal Government Customer requires on-site support at such customer's locations pursuant to contracts for subscription and support services for In-Scope Software Products, such support shall only be provided by Approved Personnel (see CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy).

## 5. Roles and Responsibilities

Role	Responsibility
CFIUS Security Officer	Approves and authorizes the FACL Administrator, Compliance Administrators, and Implementation Leaders Defines FACL training requirements Final review and verification of Background Verification (BGV) report when required Final approval of Information Protection Plans
Compliance Administrators (multiple)	Responsible for compliance with the CFIUS Access Control Policy for the servers, systems and applications they administer Responsible for developing and deploying Information Protection Plan for the servers, systems and applications they administer Audit access controls and certifies compliance Maintain and provide audit records
FACL Administrator	Administers the Federal Access Control List Verifies training completion records Verifies citizenship and location Approves FACL requests if all requirements are met
HR Implementation Leader	Verifies Former IBM Employee status Obtains, reviews and verifies BGV reports Provides records of citizenship and location Forwards BGV report to CFIUS Security Officer for review and verification when required
IT Implementation Leader	Maintains up-to-date CFIUS asset inventory
Implementation Leaders (multiple)	Validate FACL requests based on business need Approve Information Protection Plans
Legal Implementation Lead	The Legal CFIUS Implementation Lead shall ensure that third-party entities with access to the Secure Software Build Environment or U.S. Federal Government Customer Data are notified of their obligations prior to entering into a definitive agreement with HCL.

## 6. Policy Details and Procedures


### 6.1 Third-Party Contractual Requirements

Third-party entities (other than IBM), including partners, suppliers, vendors, and subcontractors with access to the Secure Software Build Environment or U.S. Federal Government Customer Data, must meet specific contractual requirements including, but not limited to:

- Restrictions on access to and security of U.S. Federal Government Customer Data
- Restrictions on access to and security of the Secure Software Build Environment
- Prompt reporting of security incidents including unauthorized disclosure of U.S. Federal Government Customer Data or unauthorized access to the Secure Software Build Environment

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	<b>CFIUS Security Policies</b>	DOC.NO. CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO. 1.00 DATE 15-Jan-2020 PAGE NO. 27 of 93

- Cooperation in connection with any review or audit pursuant to HCL's obligations under the National Security Agreement
- Record retention requirements consistent with CFIUS010 - CFIUS Governance, Oversight, and Notification Policy
- Periodic certification of compliance with such requirements

The Legal CFIUS Implementation Lead shall ensure that third-parties with access to the Secure Software Build Environment or U.S. Federal Government Customer Data are notified of their obligations prior to entering into a definitive agreement with HCL. Appropriate amendments to non-disclosure agreements, contracts, and other third-party agreements must be put in place to ensure that third-parties understand and are committed to comply with these obligations.

Third-party Personnel who require access to the Secure Software Build Environment shall be onboarded as HCL Contractors. Third-party Personnel who are approved on the Federal Access Control List are Approved Personnel and may be granted access to the Secure Software Build Environment pursuant to the requirements of 4.2.1 Access by Approved Personnel. Third-party Personnel who are Non-Approved Personnel may be granted access to the Secure Software Build Environment pursuant to the requirements of Section 4.2.3 Access by Non-Approved Personnel.

## 6.2 Federal Access Control Lists

The roles and responsibilities of Approved Personnel shall be managed via the Federal Access Control List based on the function performed by the Personnel. The Federal Access Control List will include the following functions:

FACL Function	FACL Code	Description
U.S. Federal Government Customer On-Site Support	USFG-OSS	Team members granted access permissions to provide on-site support to U.S. Federal Government Customers at concerned customer locations, pursuant to contracts for subscription and support services for In-Scope Software Products. Includes access permissions to U.S. Federal Government Customer Data and the U.S. Federal Government Support Environment.
Secure Software Build Environment Management	SSBE-MGT	Team members granted access permissions to manage the Secure Software Build Environment.
Secure Engineering Framework Testing Supervision	SEFT-SUP	Team members who supervise the Secure Engineering Framework Testing Flows.
U.S. Federal Government Customer Data Access	USFG-CDA	Team members granted access permissions to U.S. Federal Government Customer Data, including the U.S. Federal Government Support Environment.


## 6.3 Requirements for FACL Approval

The following requirements must be met for approval on the FACL.

Requirements
--------------

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	28 of 93

FACL Code	Business Need	U.S. Citizenship & Location	Training	Background Check	FACL Administrator Approval
<b>USFG-OSS</b>	Yes	Yes	Yes	Yes, except Former IBM Employees who worked on the In-Scope Software Products during their tenure with IBM at the same level of access control.	Yes
<b>SSBE-MGT</b>	Yes	Yes	Yes	Yes, except Former IBM Employees who worked on the In-Scope Software Products during their tenure with IBM at the same level of access control.	Yes
<b>SEFT-SUP</b>	Yes	Yes	Yes	No	Yes
<b>USFG-CDA</b>	Yes	Yes	Yes	No	Yes

## 6.4 Procedure for FACL Approval

The procedure for approval of an individual to be listed on the FACL is described below. This procedure may be implemented manually or may be automated.

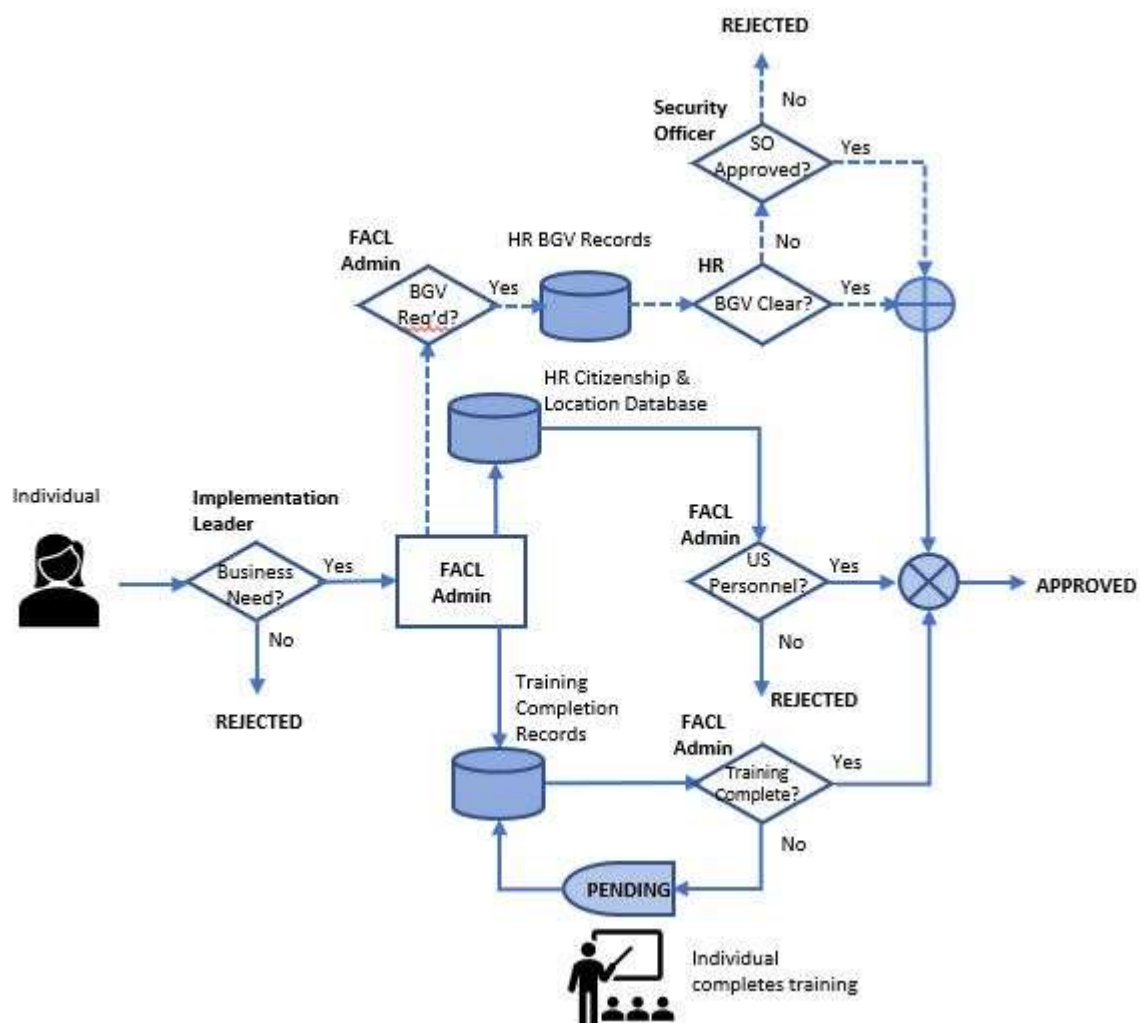
1. An individual submits a FACL authorization request to the appropriate Implementation Leader for review. An individual may submit a FACL authorization request on behalf of themselves or on behalf of another person.
2. The Implementation Leader reviews the FACL authorization request and validates or denies the request based on business need.
3. After validation by the Implementation Leader, the FACL authorization request moves to the pending state and is forwarded to the FACL Administrator.
4. The FACL Administrator verifies training completion by checking the individual's training completion records. Acceptable training completion records include, but are not limited to, reports from the corporate Learning Management System and screenshots showing successful completion of the training. The FACL authorization request shall remain in the pending state until the individual completes the required training and the FACL Administrator verifies training completion.
5. The FACL Administrator verifies the individual's Citizenship and Location based on information from the corporate HR database:
  - a. Citizenship – must be U.S.
  - b. Location – must be U.S.
 If one or both criteria are not met, the FACL request is rejected.
6. The FACL Administrator must determine whether a background check is required and, if so, notify the HR Implementation Leader.
7. If a background check is required, the HR Implementation leader verifies whether the individual is a Former IBM Employee. If so, the HR Implementation Leader verifies whether the Former IBM Employee worked on the In-Scope Software Products during their tenure with IBM at the same level of access control. If so, no background check shall be required for the individual.
8. If a background check is required, and the individual is not a Former IBM Employee or did not work on the In-Scope Software Products during their tenure with IBM at the same level of access control, the HR Implementation Leader obtains a copy of the individual's BGV report and reviews the BGV report (see CFIUS080 - CFIUS Background Verification Policy). If any required checks are missing, the HR Implementation Leader must order the incremental checks and obtain the results before proceeding.
  - a. If the BGV report includes all required checks, the BGV results are clear (Green/Amber and any discrepancies have been cleared by the BGV Council), the HR Implementation Leader verifies the BGV report.


Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

<b>HCL</b>	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	29 of 93

- b. If the BGV report is not clear (Red/Amber and/or any discrepancies have not been cleared by the BGV Council), the HR Implementation Leader forwards the BGV report to the HCL CFIUS Security Officer. The HCL CFIUS Security Officer reviews the BGV report and either finds the BGV results acceptable for approval on the FACL or rejects the FACL request.
  9. The FACL authorization request is approved by the FACL Administrator only after:
    - a. Verification of training completion
    - b. Verification of U.S. citizenship and U.S. location
    - c. If a background check is required, verification of the BGV report
  10. The FACL Administrator adds the individual to the FACL. Access to the system or information is not permitted until the individual is added to the FACL.
  11. FACL approval shall require annual re-certification of business need by the Implementation Leader.



	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	30 of 93

## 6.5 FACL Removal and Reconciliation

The FACL removal procedure shall be followed when an individual no longer has a business need for access, no longer meets the requirements for access (for example, moves outside of the U.S.), or ceases to be employed or otherwise engaged by HCL or a U.S. subsidiary of HCL for professional or technical services.

The procedure for removal from the FACL is described below. This procedure may be implemented manually or may be automated.

1. Following an event that disqualifies an individual for membership on the FACL, the individual or his/her reporting manager must promptly submit a FACL removal request to the appropriate Implementation Leader for approval. An individual may submit a FACL removal request on behalf of themselves or on behalf of another person.
2. The Implementation Leader reviews the FACL removal request and approves removal from the FACL or determines that a disqualification event did not actually occur and rejects the FACL removal request.
3. After approval of FACL removal by the Implementation Leader, the FACL removal request moves to the pending state and is forwarded to the FACL Administrator.
4. The FACL Administrator removes the individual from the FACL. (Note that the Compliance Administrators are responsible for implementing procedures to ensure that access control lists for servers, systems and applications are periodically audited to ensure consistency with the Federal Access Control List as described in Section 6.7.)


In addition, the FACL Administrator must conduct a periodic reconciliation review of the FACL to verify that all Personnel on the FACL are employed or otherwise engaged by HCL or a U.S. subsidiary of HCL for professional or technical services. Any Personnel found to be inactive must be removed from the FACL.

## 6.6 CFIUS Asset Inventory

The IT Implementation Leader must maintain an up-to-date asset inventory of all servers, systems, and applications comprising the Secure Software Build Environment, the Federal Support Environment and/or containing U. S. Federal Government Customer Data (see Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products). The CFIUS asset inventory must include, at a minimum:

1. Unique asset identifier
2. Asset name (fully qualified domain name if applicable)
3. Asset description
4. Asset location
5. Asset purpose/function
6. Asset status
7. The type(s) of information stored in or accessible from the asset, including:
  - a. U.S. Federal Government Customer Business Identifiable Information
  - b. U.S. Federal Government Customer Support Records
  - c. Source Code Repository
  - d. Build Environment
  - e. Publication Repository
  - f. SSBE Application Server
8. Access restrictions, including:
  - a. FACL Access Only (all access is restricted to Approved Personnel on the FACL)
  - b. FACL Admin Only (administrative access is restricted to Approved Personnel on the FACL)
9. Name and SAP ID of Compliance Administrator



	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	31 of 93

## 6.7 Access Controls for Servers, Systems, and Applications

Access to servers, systems and applications comprising the Secure Software Build Environment, the Federal Support Environment and/or containing U. S. Federal Government Customer Data shall be controlled as follows:

1. A Compliance Administrator must be assigned for each server, system and application with the responsibility to develop, document, and implement an Information Protection Plan for compliance with the CFIUS Access Control Policy.
2. The Information Protection Plan must be approved by the Implementation Leader and the CFIUS Security Officer.
3. The Information Protection Plan must address the following topics:
  - a. Training for users of the server, system or application
  - b. Implementation of electronic access controls or other mechanisms to limit access to Approved Personnel
  - c. Provisions for monitoring the server, system or application to detect successful or unsuccessful unauthorized access attempts or other security events.
  - d. Procedures for periodic audits of access control lists for the server, system or application to ensure consistency with the Federal Access Control List
  - e. Maintaining records of compliance and providing access to these records to the CFIUS Security Officer and Third-Party Monitor
4. All Personnel with access to servers, systems and applications comprising the Secure Software Build Environment, the Federal Support Environment and/or containing U. S. Federal Government Customer Data shall be trained on the policies and procedures for handling such information. This training must address:
  - a. Rules regarding the safeguarding of information, including restrictions on information sharing
  - b. Rules and procedures for obtaining access, determining when access is no longer required, and removal of access permissions

## 7. Audit & Record-Keeping

### 7.1 Federal Access Control List

The FACL Administrator and the HR Implementation Leader shall maintain the Federal Access Control List as described in Sections 6.4 and 6.5.

Records:

1. Federal Access Control List (FACL Administrator)
2. FACL approval requests and their disposition (FACL Administrator)
3. Citizenship and location records for Approved Personnel (HR Implementation Leader)
4. Verified background screens for Approved Personnel (HR Implementation Leader)
5. Former IBM Employee status records for Approved Personnel (HR Implementation Leader)
6. Training completion records for Approved Personnel (FACL Administrator)
7. FACL reconciliation report (FACL Administrator)


### 7.2 CFIUS Asset Inventory

As described in Section 6.6, the IT Implementation Leader shall maintain an up-to-date asset inventory of all servers, systems, and applications comprising the Secure Software Build Environment and/or containing U. S. Federal Government Customer Data.

Records:

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	32 of 93

1. Asset inventory including all CFIUS assets with required attributes (IT Implementation Leader)
2. Asset inventory change management procedure document (IT Implementation Leader)
3. Asset inventory change records (IT Implementation Leader)

### 7.3 Access Controls for Servers, Systems and Applications

As described in Section 6.7, the Compliance Administrator of each server, system, and application comprising the Secure Software Build Environment, the Federal Support Environment and/or containing U. S. Federal Government Customer Data must develop, document, and implement an Information Protection Plan for compliance with the CFIUS Access Control Policy.

Records:


1. Information Protection Plan documents including the required contents (Compliance Administrators)
2. Access control lists for the servers, systems and applications (Compliance Administrators)
3. Security event logs or other monitoring records (Compliance Administrators)
4. Periodic audit records (Compliance Administrators)

## 8. Related Documents

The following related documents are associated with this policy:


1. CFIUS001 - Glossary of Terms Related to CFIUS Security Policies
2. CFIUS010 - CFIUS Governance, Oversight, and Notification Policy
3. CFIUS030 - CFIUS Product Integrity Policy
4. CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy
5. CFIUS050 - CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment
6. CFIUS060 - CFIUS Physical Security Policy
7. CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers
8. CFIUS080 - CFIUS Background Verification Policy
9. Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	33 of 93

## 9. Change Log

Version	Date	Author(s)	Summary of Changes
1.00	December 18, 2019	Karen Plonty	Final document
1.00	January 15, 2020	Karen Plonty	Approved by CFIUS Governance Committee without changes.


	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	34 of 93

# CFIUS030

## CFIUS Product Integrity Policy

Version 1.01

Date: 07 January 2020

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	35 of 93

## 1. Purpose

The purpose of this document is to describe the implementation of the product integrity requirements of the of the National Security Agreement made among HCL, International Business Machines (“**IBM**”), and the U.S. Government.

## 2. Scope

This policy applies to all HCL Personnel involved in:

- Source Code Development for the In-Scope Software Products
- Operation of the Secure Software Build Environment
- Oversight of the Secure Engineering Framework Test Flows for the In-Scope Software Products

This policy applies to all Releases of the In-Scope Software Products. In addition, this policy applies to all Test Fixes delivered to U.S. Federal Government Customers.

This policy does not apply to products that are not In-Scope Software Products that are included in multi-product offerings along with In-Scope Software Products, subject to the CFIUS Security Officer's discretion in accordance with the CFIUS010 – CFIUS Governance, Oversight and Notification Policy.

## 3. Definitions

Capitalized terms used herein and not otherwise defined have the meaning set forth in the Glossary (CFIUS001 - Glossary of Terms Related to CFIUS Security Policies).

## 4. Policy Statement

It is HCL’s policy that:

The Secure Software Build Environment must be located exclusively in the United States and must be managed solely by Approved Personnel, as described in CFIUS020 – CFIUS Access Control Policy.

All Releases of the In-Scope Software Products must follow the Secure Engineering Framework Testing Flows under the supervision of Approved Personnel (see Appendix C).

Only Approved Personnel shall be authorized to transfer Release images of the In-Scope Software Products to Publication Repositories for U.S. Federal Government Customers.

HCL shall facilitate product integrity testing and Source Code review by the Third-Party Monitor conducted in accordance with the Agreement and in coordination with the CFIUS Security Officer, as described in CFIUS010 – CFIUS Governance, Oversight, and Notification Policy.


## 5. Roles and Responsibilities

### *Development Director*

The Development Director is the immediate executive leader of a development team responsible for an In-Scope Software Product Release, and the individual to whom the Development Managers for a Release are accountable.

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	36 of 93

The Development Director shall ensure the Source Code for their business scope is appropriately organized into compartments with controlled access.

### *Development Manager*

The Development Manager is the immediate personnel manager of development team members contributing to a Release of an In-Scope Software Product. The Development Manager is accountable to the Development Director. The Development Manager shall ensure that all Source Code is produced by Development Engineers based in locations on the International Development Locations Inventory (see Appendix C).

### *Development Engineers*

Development Engineers produce Source Code in accordance with the HCL Software Release Management Policy and Process document. The Development Engineers are accountable to a Development Manager. Irrespective of title, Development Engineers include all individuals whose responsibilities require read or write access to the Source Code of the In-Scope Software Products, whether for the purposes of development, test, or support. Development Engineers shall be based in locations on the International Development Locations Inventory.

### *Product Implementation Leader*

The Product Implementation Leader is approved by the CFIUS Security Officer to ensure compliance with the CFIUS Security Policies for In-Scope Software Products in their area of responsibility (see CFIUS010 – CFIUS Governance, Oversight and Notification Policy). The Product Implementation Leader has primary responsibility for implementation of CFIUS Security Policies and procedures under the direction of the CFIUS Security Officer. The Product Implementation Leader, in coordination with the CFIUS Security Officer, must ensure that CFIUS approval is obtained before engaging any new Third-Party Entity Service Providers to assist with the Source Code Development Process.

### *Release Manager*

The Release Manager is responsible for tracking the execution of Release plans in accordance with the HCL Software Release Management Policy and Process document. The Release Manager is responsible for leading the change management process of the Source Code Development Process for In-Scope Software Products and the Secure Engineering Framework Testing Flows through the Development Process - Change Control Task Force (DP-CCTF).


## **6. Policy Details and Related Procedures**

### **6.1 Integrity of Development Processes**

#### *Source Code Development Process and Secure Engineering Framework Testing Flows*

HCL shall maintain a documented description of its practices related to the Source Code Development Process for In-Scope Software Products. These practices are documented in the HCL Software Release Management Policy and Process document, which describes the processes for planning, designing, developing, testing, and deploying Releases for the In-Scope Software Products, including the Secure Engineering Framework Testing Flows.

HCL may, from time to time, update the Source Code Development Process and the Secure Engineering Framework Testing Flows to reflect business necessities and changes of circumstance, ensuring that the Source Code Development Process and Secure Engineering Framework Testing Flows remain consistent with the Agreement. The Development Process Change Control Task Force (DP-CCTF) shall manage, oversee and approve changes to

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	37 of 93

the Source Code Development Process and the Secure Engineering Framework Testing Flows. The DP-CCTF will be led by the Release Manager.

Prior to granting final approval to any proposed change to the Source Code Development Process or the Secure Engineering Framework Testing Flows, the DP-CCFT shall, in coordination with the CFIUS Security Officer, submit the proposed changes to the CFIUS Monitoring Agencies for approval. If the CFIUS Monitoring Agencies do not object to such changes in writing within fifteen (15) business days of notice, then non-objection shall be presumed and the change shall be implemented. If the CFIUS Monitoring Agencies object, the proposed change will not be made.

### *Third-Party Entity Service Providers*

The Product Implementation Leader shall maintain the Third-Party Entity Service Provider Inventory in Appendix A to this policy, as updated from time to time in accordance with the Agreement, which catalogs the Third-Party Entity Service Providers (other than IBM) engaged by HCL to assist in the Source Code Development Process for the In-Scope Software Products. This inventory shall include, at a minimum, the entity's name and primary business address along with a description of the entity's role and responsibility as it pertains to the Source Code Development Process. Third-party entities who are not listed on the Third-Party Entity Service Provider Inventory shall not be engaged by HCL to assist with the Source Code Development Process.

The Third-Party Entity Service Provider Inventory shall include:

- Outsourced service providers, such as companies engaged by HCL to provide software which they design, develop, and test under their own management supervision
- Third-party product testing or verification services, including but not limited to product penetration testing
- Customer support services provided to U.S. Federal Government Customers by a third-party company

Third-party entities with no involvement in the Source Code Development Process shall not be included in the Third-Party Entity Service Provider Inventory:

- Companies that provide commercially available software products bundled with or integrated into the In-Scope Software Products
- Staff augmentation firms that provide staff who are managed by HCL managers and integrated into HCL's internal processes

The Product Implementation Leader must notify the CFIUS Security Officer 45 calendar days before entering into an agreement with any new third-party entity to assist with the Source Code Development Process for the In-Scope Software products. The CFIUS Security Officer must submit the proposed changes to the Third-Party Entity Service Provider Inventory to the CFIUS Monitoring Agencies for approval, consistent with CFIUS010 – CFIUS Governance, Oversight, and Notification Policy. If the CFIUS Monitoring Agencies do not object in writing within fifteen (15) business days of notice, then non-objection shall be presumed and the change shall be implemented. If the CFIUS Monitoring Agencies object, the proposed change will not be made. The Third-Party Entity Service Provider Inventory may not be updated and the Third-Party Entity Service Provider may not be engaged until expressly approved by the CFIUS Security Officer.


## **6.2 Source Code Development**

All Source Code for the In-Scope Software Products must be developed only by Development Engineers working from locations listed in Appendix B: International Development Locations Inventory, attached to this policy. HCL shall update the International Development Locations Inventory in accordance with CFIUS010 - CFIUS Governance, Notification, and Oversight Policy.

Copies of all Source Code for the In-Scope Software Products shall be submitted to Source Code Repositories located in the United States and managed by Approved Personnel, as described in the CFIUS020 - CFIUS Access

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	38 of 93

Control Policy.

Development Managers shall request access to Source Code Repositories only for Development Engineers working from locations listed on the International Development Locations Inventory. Development Managers shall revalidate access for any Development Engineer who changes work location and shall ensure access is revoked, if needed. Development Directors shall perform periodic review of Source Code access by geography for their business scope, at least once per quarter.

Development Engineers shall not develop or submit source code to the Source Code Repositories when traveling outside of locations listed on the International Development Locations Inventory.

Development Engineers' read and/or write access to the Source Code Repositories shall be limited to only the Source Code necessary for their respective scope of work and role. Development Directors shall ensure appropriate compartmentalization for the Source Code for their business scope and shall review access by compartment quarterly.

Development Engineers' access to the executable code and object code artifacts from Production Build Servers shall be limited to read access privileges for the components required for further Source Code development within their respective scope of work and role (see Section 6.4).

### 6.3 Source Code Servers and Repositories

Source Code Repositories shall be housed on servers located in the United States. Only Approved Personnel shall have server-level access privileges to the servers housing the Source Code Repositories. For the avoidance of doubt, Development Engineers shall have read and/or write access to the Source Code Repositories housed on such servers, as described in the previous section.

The Source Code Repositories shall be managed solely by Approved Personnel.

Only Approved Personnel shall select the Source Code for a Release of an In-Scope Software Product. Only Approved Personnel shall be able to make modifications to the selected Source Code once Approved Personnel have selected the Source Code for a Release of an In-Scope Software Product.

Changes to Source Code servers and Source Code Repositories shall be managed through a documented change control process CFIUS050 – CFIUS Security Policy for the SSBE, including:

- Changes in server-level access privileges
- Changes in access to Source Code Repositories

### 6.4 Production Build Servers


Production Build Servers shall be housed exclusively in the United States and managed exclusively by Approved Personnel. Production Build Servers in the United States shall be used for building all Releases and all Test Fixes delivered to U.S. Federal Government Customers. Test Fixes for commercial customers may be built and delivered by development and/or support engineers in multiple geographies outside the Secure Software Build Environment, as needed to deliver Test Fixes to commercial customers in a timely fashion.

Only Approved Personnel shall have access privileges and configuration modification rights to the Production Build Servers.

Only Approved Personnel on the Federal Access Control List will have the ability to select the source code and initiate the build process for any Release of an In-Scope Software Product and for any Test Fix delivered to U.S.

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	39 of 93

Federal Government Customers. After the build process is initiated by Approved Personnel, non-U.S. Personnel may initiate test jobs to test any Release, or any Test Fixes for U.S. Federal Government Customers, and may monitor test results.

Only Approved Personnel shall have privileges to transfer the Release of an In-Scope Software Product from Production Build Servers to Publication Repositories for U.S. Federal Government Customers.

Build automation servers hosting scripts and/or tools used to control the production of a Release by the Production Build Servers shall be housed exclusively in the United States and managed exclusively by Approved Personnel. Only Approved Personnel shall have access privileges and configuration modification rights to build automation servers and tools. Changes to these servers and tools shall be managed as documented in CFIUS050 – CFIUS Security Policy for the SSBE.

Changes to Production Build Servers and build automation servers tools shall be managed through a documented change control process CFIUS050 – CFIUS Security Policy for the SSBE, including:

- Changes to server-level access privileges
- Changes to build automation privileges

## 6.5 Publication Servers and Publication Repositories

Publication servers hosting Publication Repositories for U.S. Federal Government Customers must be housed exclusively in the United States, and Publication Repositories for U.S. Federal Government Customers shall be managed by Approved Personnel.

Only Approved Personnel shall have administrative access privileges and configuration change rights to the Publication Repositories for U.S. Federal Government Customers. Those privileges must be granted consistent with the CFIUS020 - CFIUS Access Control Policy.

## 6.6 Secure Engineering Framework Testing Flows


Secure Engineering Framework Testing Flows shall follow Appendix C and the practices outlined in the HCL Software Release Management Policy and Process document.

### 6.6.1 Source Code Scanning

- All Releases shall undergo static source code scanning and open source binary scanning with approved scanning tools to identify vulnerabilities in the product code and bundled open source software libraries.
- Scan results shall be reviewed by Approved Personnel to ensure that high severity issues are resolved, confirmed as not applicable, or have an approved mitigation plan prior to publication of the Release.

### 6.6.2 Penetration Testing

- Penetration testing shall be conducted annually on In-Scope Software Products by a penetration testing team comprised of Approved Personnel.
- Penetration test results shall be reviewed by Approved Personnel to ensure high severity issues are resolved, confirmed as not applicable, or have an approved mitigation plan prior to publication of a subsequent Release.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	40 of 93

### 6.6.3 Script and Content Publication Testing

- Includes content that is not source code and cannot be scanned by static scanning tools, such as and not limited to scripts, catalog data, configuration files, etc.
- Approved Personnel shall perform visual review and inspection of scripts and content
- High severity issues shall be resolved, confirmed as not applicable or have an approved mitigation plan prior to a Release.

### 6.7 Third-Party Monitor Production Integrity Testing

Consistent with the CFIUS010 - CFIUS Governance, Notification, and Oversight Policy, HCL shall retain a Third-Party Monitor to arrange for product integrity testing of a subset of In-Scope Software Products. Such testing shall be conducted in consultation with the CFIUS Security Officer.

The specific products and testing scope and methodology for such products shall be agreed upon by the Third-Party Monitor and the CFIUS Security Officer, and shall be submitted to the CFIUS Monitoring Agencies at least thirty (30) calendar days before the test. Such scope and methodology may include the participation of additional parties, subject to such parties' subordination to the Third-Party Monitor and the approval of the CFIUS Monitoring Agencies. If the CFIUS Monitoring Agencies fail to object within that time period, non-objection shall be presumed. Any objections by the CFIUS Monitoring Agencies shall be addressed by HCL to the CFIUS Monitoring Agencies' satisfaction.

### 6.8 Third-Party Monitor Source Code Reviews

Only when requested by the CFIUS Monitoring Agencies, the Third-Party Monitor shall arrange for review of the Source Code for a sample of the In-Scope Software Products through a process and plan agreed upon through consultation with the CFIUS Security Officer and the CFIUS Monitoring Agencies. Such testing shall be conducted in consultation with the CFIUS Security Officer.

## 7. Audit & Record-Keeping

### 7.1 Source Code Development Process Change Management Records

The Release Manager shall maintain records of prior CFIUS approval for all changes to the HCL Software Release Management Policy and Process document and the Secure Engineering Framework Testing Flows.

### 7.2 Third-Party Service Providers Change Records

The Product Implementation Leader shall maintain records of prior CFIUS approval for all changes to the Third-Party Entity Service Provider Inventory.


### 7.3 Source Code Compartmentalization Records

Source code compartmentalization records shall be maintained by the Development Directors. These records shall be made available to CFIUS and the Third-Party Monitor upon request.

### 7.4 Secure Engineering Framework Testing Flow Records

Secure Engineering Framework Testing records shall be maintained for each Release in accordance with the Secure Engineering Framework Testing Flow process.



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	41 of 93

## 8. Related Documents


1. HCL Software Release Management Policy and Process
2. CFIUS001 - Glossary of Terms Related to CFIUS Security Policies
3. CFIUS010 – CFIUS Governance, Oversight and Notification Policy
4. CFIUS020 – CFIUS Access Control Policy
5. CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy
6. CFIUS050 - CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment
7. CFIUS060 - CFIUS Physical Security Policy
8. CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers
9. CFIUS080 - CFIUS Background Verification Policy

## 9. Change Log

Version	Date	Author(s)	Summary of Changes
1.00	December 18, 2019	Pat Guido Margaret Rora Shailaja Golikeri Shahar Sperling	Final document
1.01	January 7, 2020	Karen Plonty	Added Mexico to International Development Locations Inventory based on email approval from the CFIUS Monitoring Agencies on December 20, 2019.
1.01	January 15, 2020	Karen Plonty	Approved by CFIUS Governance Committee without changes.

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	42 of 93


## Appendix A: Third-Party Entity Service Provider Inventory

Version 1.1, August 14, 2019


No.	Name	Business Address	Role and Responsibility
1	Below0Day	1600A N. Jackson St. Milwaukee, WI 53202	Penetration testing
2	BrowserStack	444 De Haro Street, Suite 212, San Francisco, CA 94107	Testing platform that provides access to a wide variety of device types and desktop browsers via their cloud platform.
3	Cherwell	10125 Federal Drive, Suite 100 Colorado Springs, CO 80908	Contributor to third party software catalog.
4	Cornerstone Technology Partners	Cornerstone Technology Partners Inc. d/b/a Epilio 33 Broad Street, 5th Floor Boston, MA 02109	Create a replacement for the existing discussions and teamroom templates with a focus on Notes client.
5	Flexera	300 Park Blvd., Suite 500 Itasca, IL 60143	License and subscription management.
6	IBA	2583/13 Petržilkova St. Prague 5, 15800 Czech Republic	Assist in testing for Digital Experience product.
7	Immix	1602 Village Market Blvd SE, Suite 215 Leesburg, VA 20175	License / subscription support for federal customers.
8	Nash.com	Weidenweg 58 40723 Hilden Germany	Assist in the testing of Note/Domino product line.
9	Topcoder	201 S. Capitol Ave., Suite #1100 Indianapolis, IN 46225	Runs design and development challenges on their crowdsourcing platform. The best of the challenge is considered for inclusion in the product.
10	Uilicious	67 Ubi Road 1 #08-15 Oxley Bizhub 1 Singapore 408730	Solution for teams to rapidly set up end-to-end user tests and continuously monitor their web application using cloud platform.
11	WeLocalize	123 NE 3rd Ave #209 Portland, OR 97232	Globalization of product releases.
12	WhiteSource	79 Madison Ave New York, NY 10016	OpenSource software scanning tool.
13	HackerOne	33 Irving Pl New York, NY 10003, USA	Provide product security vulnerability assessment, management and reporting services.
14	TimeToAct Group	Im Mediapark 5, 50670 Köln, Germany	Business partner who will engage in subcontracting of development work around IBM Connections Engagement Center (ICEC).

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	<b>CFIUS Security Policies</b>	DOC.NO. CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO. 1.00 DATE 15-Jan-2020 PAGE NO. 43 of 93

No.	Name	Business Address	Role and Responsibility
15	Universität Koblenz-Landau	Rhabanusstr. 3, 55118 Mainz, Germany	Research projects around network analysis within Connections.
16	Vegard IT GmbH	Genter Str. 64, 13353 Berlin, Germany	Co-development of specific customer solutions built on Connections.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	44 of 93

## Appendix B: International Development Locations Inventory

### Development Locations:

United States  
 Italy  
 India  
 Canada  
 Israel  
 France  
 Germany  
 United Kingdom  
 Philippines  
 Japan  
 Poland  
 Australia  
 Singapore  
 Mexico

### Support Hotline (U.S. Federal Government Customers):

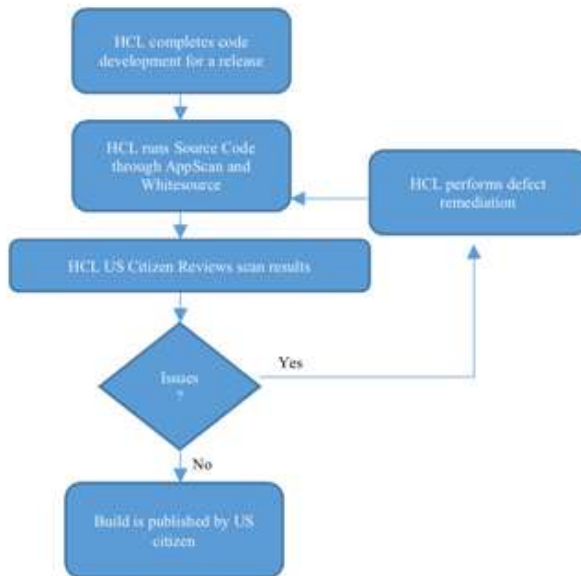
United States

<b>HCL</b>	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	45 of 93

## Appendix C: Secure Engineering Framework Testing Flows

### a) Source Code Scan Release Flow


#### Source Code Scan Release Flow



The Source Code scan release flow is followed for releases with compiled object code.

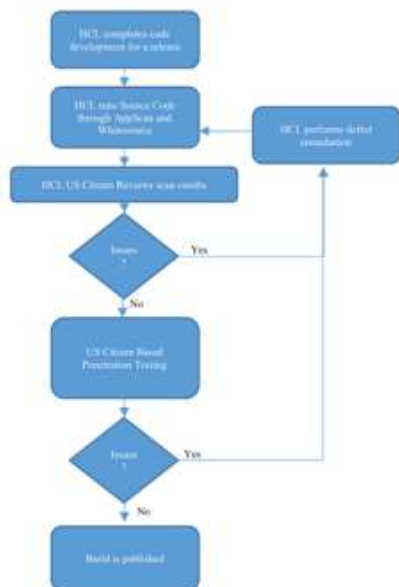
#### Source Code Scan Release Process:

1. HCL will source scan (e.g., AppScan) and open source scan (e.g., WhiteSource) the code before a code release.
2. HCL US Citizen engineer(s) will validate and verify the scanning and results of the scan.
3. High Severity issues associated with the scan will be dispositioned prior to release.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	46 of 93

## b) Penetration Testing Release Flow

### Penetration Testing Release Flow

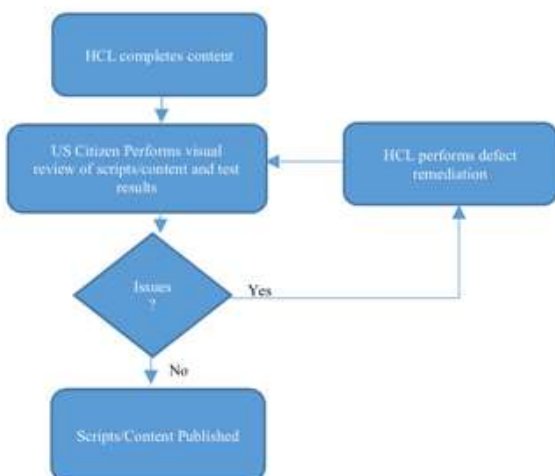


The penetration testing release flow is followed annually for releases with compiled object code. Penetration Testing Release Process:

1. HCL will source scan (e.g. AppScan) and open source scan (e.g., WhiteSource scan) the code before a code release.
2. HCL US Citizen engineer(s) will validate and verify the scanning and results of the scan.
3. High Severity issues associated with the scan will be dispositioned, and code rescanned.
4. Build is delivered to a US citizen penetration testing team prior to release.
5. High Severity issues identified by the penetration testing are dispositioned prior to release.

## c) Script and Content Publication Flow


### Script and Content Publication Flow



This process is followed for scripting and content releases, where automated tools are not available.

Script and Content Publication Flow:

1. HCL US Citizen engineer(s) will perform a visual review and inspection of the scripts and content.
2. High Severity issues associated with the review will be dispositioned prior to release.


	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	47 of 93

# CFIUS040

## CFIUS U.S. Federal Government Customer Support and Data Protection Policy

Version 1.00

Date: 18 December 2019

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	48 of 93

## 1. Purpose

The purpose of this policy is to implement the U.S. Federal Government Customer Data protection requirements and the U.S. Federal Government Customer support requirements of the National Security Agreement made among HCL, International Business Machines (“IBM”), and the U.S. Government.

## 2. Scope

This policy applies to all HCL Personnel who may have access to U.S. Federal Government Customer Data, including but not limited to the Personnel involved in the operation of the HCL Federal Support Center (“FSC”) providing both routine and emergency technical support for In-Scope Software Products to U.S. Federal Government Customers.

## 3. Definitions

Capitalized terms used herein and not otherwise defined have the meaning set forth in the Glossary (CFIUS001-Glossary of Terms Related to CFIUS Security Policies).

**“Customer Data Repository” or “CuDaR”** means the secure data storage location where customer data is stored. The CuDaR also has a customer facing portal where the customer may upload diagnostic data during any requested support case activities.

**"FSC Software Support Engineer"** means a member of the Federal Support Center who processes a U.S. Federal Government Customer support case.

**"Level 3 Software Development Team"** means a Level 3 development organization that develops Test Fixes and/or Releases for the In-Scope Software Products in support of customer problems, complaints or suggestions.

## 4. Policy Statement


It is the policy of HCL that:

HCL shall safeguard U.S. Federal Government Customer Data by restricting access to U.S. Federal Government Customer Data to only Approved Personnel.

HCL shall ensure U.S. Federal Government Customer support requests are received only by Approved Personnel, and handled within a ticketing tool dedicated to U.S. Federal Government Customers and accessible only to Approved Personnel.

Any on-site support at a U.S. Federal Government Customer’s location pursuant to contracts for subscription and support services for In-Scope Software Products shall be provided only by Approved Personnel.



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	49 of 93

The CFIUS Security Officer shall notify the CFIUS Monitoring Agencies within twenty-four (24) hours of making a determination that there has been a Known Breach involving any breach or unauthorized disclosure of U.S. Federal Government Customer Business Identifiable Information or U.S. Federal Government Customer Support Records in violation of HCL's CFIUS Security Policies, as further described in CFIUS010 - CFIUS Governance, Oversight, and Notification Policy.

## 5. Roles and Responsibilities

### Federal Support Implementation Leader

- Maintains compliance audit records as defined in Section 7
- Provides business records upon request by the CFIUS Security Officer, Third-Party Monitor and/or Third-Party Auditor
- Serves as primary contact in the Federal Support Center for reports of Suspected Breaches
- Supports Suspected Breach investigations

### Federal Support Environment Compliance Administrator

- Responsible for the operation, maintenance and support of the Customer Data Repository and the electronic ticket system used to document support cases opened by U.S. Federal Government customers for technical assistance with any of the In-Scope Software Products.
- Grants and removes access to the Federal Ticket System and the Federal Customer Data Repository (CuDaR)
- Maintains compliance audit records as defined in Section 7

### FSC Level 1 Software Support Engineer

- Approved Personnel who engage with U.S. Federal Government Customers to address anomalies reported on the supported software applications to which the customer is entitled.
- Assist with U.S. Federal Government customer case creation as necessary.
- Provide initial triage, perform case documentation, and attempt first-call resolution for inquiries submitted by customers.
- Provide case status updates to customers as necessary during the lifetime of active cases.
- Document customer satisfaction with case resolution and close support cases once issues are confirmed resolved.
- Verify deletion of customer provided diagnostic data gathered and stored in the Customer Data Repository (CuDaR) Secure File Transport Protocol (SFTP) repository upon resolution and closure of customer support cases.


### FSC Level 2 Software Support Engineer

- Approved Personnel who provide in depth investigation and research to attempt to resolve cases for customer issues.
- Gather necessary diagnostic test or log information to append to cases submitted to Level 3 Software Development Support team for technical or developmental assistance.
- Ensures that all U.S. Federal Government Customer Data is de-identified or anonymized (by masking or substituting with anonymous aliased information) in the support case data files prior to any engagement of Level 3 Software Development Support Engineers.

### Level 3 Software Development Team

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	50 of 93

- Comprised of members who are not Approved Personnel and are not authorized to access U.S. Federal Government Data
- Responsible for developing Test Fixes and/or Releases for the In-Scope Software Products in support of customer problems, complaints or suggestions.
- Update the HCL internal software Knowledge Base as necessary to provide a historical record of the issue and the fix action.

#### **Non-Federal Level 2 Product Support Team**

- Comprised of members who are not Approved Personnel and are not authorized to access U.S. Federal Government Customer Data
- Provide additional In-Scope Software Product support to the Federal Support Center and engage the Level 3 Software Development Teams when necessary.


## **6. Policy Details and Corresponding Procedures**

### **6.1 U.S. Federal Government Customer Business Identifiable Information**

#### *Definition of U.S. Federal Government Customer Business Identifiable Information*

See CFIUS001 - Glossary of Terms Related to CFIUS Security Policies. Examples of U.S. Federal Government Customer Business Identifiable Information include, but are not limited to:

- Any reference to a U.S. Federal Government Customer (direct or end customer) agency, department, or entity name, reference, or acronym. (Note: Mere U.S. Federal Government Customer agency, department or entity names, references or acronyms alone without any further customer identifying information are not considered U.S. Federal Government Customer Business Identifiable Information if said information relates to unclassified work that is otherwise discoverable in the public domain, including through sources such as the Federal Procurement Data System or USAspending.gov.)
- Any address records identifiable as a U.S. Federal Government Customer (direct or end customer)
- Any business phone number records identifiable as associated with a U.S. Federal Government Customer (direct or end customer)
- Any personnel name records identifiable as associated with a U.S. Federal Government Customer (direct or end customer)
- Any personnel address records identifiable as associated with a U.S. Federal Government Customer (direct or end customer)
- Any personnel email address records identifiable as associated with a U.S. Federal Government Customer (direct or end customer)
- Any personnel phone number records identifiable as associated with a U.S. Federal Government Customer (direct or end customer)
- Any non-aggregated and non-anonymized unique data identifiable as related to U.S. Federal Government Customer (direct or end customer) products, service and support entitlements
- Any non-aggregated and non-anonymized data extracted from a U.S. Federal Government Customer (direct or end customer) network/application environment that contains unique information (i.e., IP address, MAC Address, Host Name, User Name, FQDN URL)

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	51 of 93

### *U.S. Federal Government Customer Business Identifiable Information Control*

Access to U.S. Federal Government Customer Business Identifiable Information will be restricted to Approved Personnel.

Approved Personnel may share U.S. Federal Government Customer Business Identifiable Information with other Approved Personnel, IBM employees and the Federal Business Partners for valid business reasons using designated channels (see U.S. Federal Government Customer Business Identifiable Information Storage and Transmission). Written approval from the CFIUS Security Officer is required before sharing such information with all other HCL Personnel and any other third-parties.

### *U.S. Federal Government Customer Business Identifiable Information Storage and Transmission*

U.S. Federal Government Customer Business Identifiable Information must be stored and transmitted exclusively within the U.S.


Written approval from the CFIUS Security Officer is required before U.S. Federal Government Customer Business Identifiable Information may be stored in any server, system, or application (including those provided by third-parties). See Appendix A for a list of approved, designated storage and transmission channels for U.S. Federal Government Customer Business Identifiable Information.

Approved Personnel may store documents or files containing U.S. Federal Government Customer Business Identifiable Information on their HCL or Federal Business Partner provided workstations provided such workstations are compliant with HCL or Federal Business Partner security policies, including but not limited to disk encryption, password protection and malware protection (for HCL provided workstations, see Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products). However, such documents and files may not be stored in any file sharing system that has not been approved by the CFIUS Security Officer, including, but not limited to, OneDrive, Microsoft Teams, Microsoft 365, or SharePoint.

## **6.2 U.S. Federal Government Customer Support Requests**

U.S. Federal Government Customer support requests for technical assistance will be accepted only via the following channels:

- HCL FSC telephone support (855) 855-5016 | (984) 333-9014
- HCL FSC web portal <https://hclpnpsupport.hcltech.com/csm?id=federal>
- HCL FSC Secure Email: [hclfederalsupport@hclgov.com](mailto:hclfederalsupport@hclgov.com)
- HCL FSC URL for customer facing ticketing system:  
<https://hclpnpsupport.hcltech.com/csm?id=federal>
- Customers contacting the FSC for non-supported accounts will be transferred or directed to the correct supporting entity.
- U.S. Federal Government Customers contacting a non-Federal supporting entity will be directed to the FSC.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	52 of 93

### *On-Site Support*

Any time a U.S. Federal Government Customer requires on-site support at such customer's location(s) pursuant to contracts for subscription and support services for In-Scope Software Products, such support will only be provided by Approved Personnel as documented in CFIUS020 – CFIUS Access Control Policy.

### *U.S. Federal Government Customer Support Records*

See CFIUS001 - Glossary of Terms Related to CFIUS Security Policies for the definition of U.S. Federal Government Customer Support Records.

Access to U.S. Federal Government Customer Support Records will be restricted to Approved Personnel.

U.S. Federal Government Customer Support Records will be stored and transmitted exclusively in the U.S. in a ticketing tool and Customer Data Repository dedicated to U.S. Federal Government Customers (the "Federal Support Environment").

Written approval from the CFIUS Security Officer is required before any U.S. Federal Government Customer Support Records will be stored in any server, system, or application (including those provided by third-parties). See Appendix A for a list of approved, designated storage and transmission channels for U.S. Federal Government Customer Support Records.

## **6.3 Development Support by Non-Approved Personnel**


Non-Approved Personnel providing development support will not be given access to any U.S. Federal Government Customer Business Identifiable Information or U.S. Federal Government Customer Support Records. Non-Approved Personnel providing development support will only be given access to de-identified and/or anonymized information that cannot be linked to a particular U.S. Federal Government Customer.

FSC support cases requiring escalation to a Level 3 Software Development Team for an In-Scope Software Product will have all U.S. Federal Government Customer Data de-identified and/or anonymized by the FSC Level 2 Software Support Engineer prior to being submitted to the appropriate non-Federal Level 2 Product Support Team via the HCL non-Federal ticketing tool. In turn, the non-Federal Level 2 Product Support Team will engage the appropriate Level 3 Software Development Team.

## **6.4 U.S. Federal Government Customer Reported Product Security Vulnerabilities**

U.S. Federal Government Customers shall be directed to report product security vulnerabilities for In-Scope Software Products by contacting the FSC through the channels described in Section 6.2.

FSC Level 2 Software Support Engineer who receives a U.S. Federal Government Customer reported support case for a product security vulnerability will first de-identify and/or anonymize any U.S. Federal Government Customer Data. The FSC Level 2 Software Support Engineer will then promptly submit the support case to the appropriate non-Federal Level 2 Software Support Team for that specific product.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	53 of 93

The FSC Level 2 Software Support Engineer shall also notify the HCL Product Security Incident Response Team following the guidance of the processes in CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers and [the HCL Software PSIRT Program page](#).

The non-Federal Level 2 Software Support Team for the product will engage the appropriate Level 3 Software Development Team to address the reported product security vulnerability. The Level 3 Software Development Team will determine a resolution to the vulnerability. The resolution will be described in a published security bulletin made available from the [Knowledge Base on the HCL Support Portal](#). If the resolution involves a Test Fix, U.S. Federal Government Customers will be directed to the Federal Support Environment where they can download the Test Fix.

## 6.5 U.S. Federal Government Customer Communication

- All email communication initiated by Approved Personnel to U.S. Federal Government Customers or containing U.S. Federal Government Customer Business Identifiable Information may only be conducted using approved email accounts (see Appendix A).
- Approved Personnel may contact U.S. Federal Government Customers via telephone, and must take reasonable precautions to ensure the privacy of the communication.
- All U.S. Federal Government Customer email communications regarding U.S. Federal Government Customer Support Requests must be conducted via email utilizing the designated FSC group email address ([hclfederalsupport@hclgov.com](mailto:hclfederalsupport@hclgov.com)).
- All online meeting, video conferencing, and/or desktop sharing tools used by HCL Personnel to initiate communication with U.S. Federal Government Customers must be approved in writing by the CFIUS Security Officer.
- U.S. Federal Government Customer provided diagnostic data and log files must be uploaded to and stored in the Federal Support Environment Customer Data Repository (CuDaR).
- U.S. Federal Government Customers will have secure URL access to the HCL FSC Support Ticket system to create, escalate, review, and approve closure of their open cases.


## 6.6 U.S. Federal Government Customer Initiated Contact

In the event a U.S. Federal Government Customer contacts HCL through other than the designated channels and procedures established by HCL, HCL will, as soon as it becomes aware of such communication, use its best efforts to re-direct the contact to the channels designated for U.S. Federal Government Customers (see Section 6.2 and Appendix A).

Although such contact alone does not constitute a Suspected Breach, the recipient of the contact must report the contact to the appropriate CFIUS Implementation Leader, who will notify the CFIUS Security Officer. The CFIUS Security Officer will report such contacts to the Third-Party Monitor and the CFIUS Monitoring Agencies as described in CFIUS010 - CFIUS Governance, Oversight, and Notification Policy.

## 6.7 HCL Customer-Facing Web Pages

Unless otherwise approved in writing by the CFIUS Security Officer, HCL customer-facing web pages with web forms that allow users to enter identifying data must implement measures to avoid collecting U.S. Federal Government Customer Business Identifiable Information from U.S. Federal Government Customers.

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	54 of 93

Any web form that allows users to enter identifying data must first require the user to acknowledge that they are not a U.S. Federal Government employee or agency, nor are they submitting information with respect to or on behalf of one, before the form data may be submitted to the server and the web page functionality may continue. The value of the user's acknowledgement must be stored with the form data. If the user does not so acknowledge, the form data containing identifying data must not be submitted to or stored on the server and the web page functionality must not continue.

Despite these measures, it still may be possible for U.S. Federal Government Customers to enter their U.S. Federal Government Customer Business Identifiable Information on these web forms by indicating that they are not U.S. Federal Government Customers during the submission process. If this circumstance were to occur, HCL shall treat such submissions as permissible exceptions as described in Section 6.8. paragraph A.ii.

## 6.8 Exceptions

The restrictions set forth in this policy with respect to the securing of U.S. Federal Government Customer Business Identifiable Information and U.S. Federal Government Support Records shall not apply to the extent that:

- A. The CFIUS Security Officer has approved in writing, and any U.S. Federal Government Customer has elected in writing to provide any U.S. Federal Government Customer Business Identifiable Information or U.S. Federal Government Customer Support Records:
  - i. To HCL Personnel who are not Approved Personnel; and/or
  - ii. Through channels other than those designated by HCL solely for receipt of such information and records, as listed in Appendix A: Designated Storage and/or Transmission Channels for U.S. Federal Government Customer Data; or
- B. Any U.S. Federal Government Customer Business Identifiable Information or U.S. Federal Government Customer Support Records is incidentally acquired by HCL through the public domain.


## 6.9 Notification

All HCL Personnel must promptly report any Suspected Breach of this policy to the Customer Support Implementation Leader (or other CFIUS Implementation Leader assigned to their organization or function) as described in CFIUS010 - CFIUS Governance, Oversight, and Notification Policy. Personnel are required to report any Suspected Breaches of this Policy, including but not limited to:

- Any suspected unauthorized access to the Federal Support Environment
- Any suspected unauthorized access to or disclosure of U.S. Federal Government Customer Business Identifiable Information or U.S. Federal Government Customer Support Records

The Customer Support Implementation Leader or other receiving CFIUS Implementation Leader shall conduct a preliminary investigation to determine whether the reported Suspected Breach may constitute a breach (including but not limited to a breach or unauthorized disclosure of U.S. Government Customer Data) or requires further review, and if so, shall promptly forward the Suspected Breach report and results of the preliminary investigation to the CFIUS Security Officer as described in as described in CFIUS010 - CFIUS Governance, Oversight, and Notification Policy.



	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	55 of 93

Upon receipt of a Suspected Breach report from the CFIUS Implementation Leader, the CFIUS Security Officer shall promptly notify the Third-Party Monitor and open an investigation to determine if the reported Suspected Breach constitutes a breach. Upon determining that any Suspected Breach constitutes a breach, such breach shall be deemed a Known Breach. If the Known Breach involves a breach or possible unauthorized disclosure of U.S. Federal Government Customer Data, the CFIUS Security Officer must notify the CFIUS Monitoring Agencies and the Third-Party Monitor of the reported Known Breach as required in CFIUS010 - CFIUS Governance, Oversight, and Notification Policy.

## 6.10 System Accesses and Termination

To request access to specific systems used to support U.S. Federal Government Customers, FSC Personnel should contact the following individuals:

- Federal Access Control List – CFIUS Security Officer
- HCL Federal Support Ticket System – Federal Support Environment Compliance Administrator
- CuDaR – Federal Support Environment Compliance Administrator

Grant of system access is contingent upon the FSC Personnel meeting all security criteria as documented in the CFIUS Background Verification Policy, having been approved on the FACL, and having a legitimate business need for access.

System access will be terminated promptly and removal from the FACL will occur promptly upon any of the following statuses:


- Personnel are reassigned out of the Federal Support Center.
- Personnel are the subject of an investigation or disciplinary action by HCL management.
- Personnel have resigned or have been terminated from employment with HCL.

Access to the HCL Federal Support Center secure work spaces (located in Cary, North Carolina and Chelmsford, Massachusetts) is limited to Approved Personnel. Access is via electronic badge swipe. Badge swipe activity is recorded and maintained by facility security management (see CFIUS060 - CFIUS Physical Security Policy). Badge access privileges and access logs shall be reviewed monthly by the Federal Support Environment Compliance Administrator.

## 7. Audit & Record-Keeping

The Federal Support Implementation Leader will maintain records of the following information for the purpose of compliance audit reporting:

- U.S. Federal Government Customer tickets – Closed tickets will be retained for audit per the retention requirements in Section 7.2.
- FSC Access Log – Badge access privileges, badge access logs, and guest logs
- Non-Federal Customer tickets created by FSC Level 2 Software Support Engineers containing de-identified or anonymized U.S. Federal Government Customer Data

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	56 of 93

## 7.1 List of U.S. Federal Government Customers by HCL Customer Number

HCL will augment all U.S. Federal Government Customer account records transferred from IBM to HCL with an HCL Customer Number and store them on the secure Federal Support Environment CuDaR.

## 7.2 U.S. Federal Government Customer Support Records

All U.S. Federal Government Customer Support Records will be maintained in the Federal Support Environment a secure, searchable U.S. Federal Government Customer ticketing database, restricted to Approved Personnel only, for a period of three (3) years. Cases will be purged once the retention period expires. Data retained after the retention period will be limited to:

- Number of cases created
- Number of cases by Severity/Priority
- Number of cases by specific software application

## 7.3 Retention of Data Uploaded to Federal Support Environment CuDaR

U.S. Federal Government Customer diagnostic data and log files uploaded to the Federal Support Environment CuDaR by the customer will be maintained for the active life of the support case. The diagnostic data and/or log files shall be purged once the associated support case is closed.

## 7.4 Data Transfers with Federal Business Partner

All new or updated U.S. Federal Government Customer Data record transfers from the Federal Business Partner to the FSC are performed by a secure upload to the Federal Support Environment CuDaR. Once the information is received from the Federal Business Partner, it is incorporated into the Customer Management Record database.

# 8. Related Documents

The following related documents are associated with this policy:


1. CFIUS001 - Glossary of Terms Related to CFIUS Security Policies
2. CFIUS010 - CFIUS Governance, Oversight, and Notification Policy
3. CFIUS020 – CFIUS Access Control Policy
4. CFIUS030 - CFIUS Product Integrity Policy
5. CFIUS050 - CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment
6. CFIUS060 - CFIUS Physical Security Policy
7. CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers
8. CFIUS080 - CFIUS Background Verification Policy
9. Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products

# 9. Change Log


Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	57 of 93

Revision	Date	Author	Description of Change
1.00	December 18, 2019	Maurice Johnson	Final document
1.00	January 15, 2020	Karen Plonty	Approved by the CFIUS Governance Committee without changes.


	CFIUS Security Policies	DOC.NO. CFIUS100
	U.S. National Security Compliance	VER.NO. 1.00 DATE 15-Jan-2020 PAGE NO. 58 of 93

## Appendix A: Designated Storage and/or Transmission Channels for U.S. Federal Government Customer Data

Type of Request or Data	Communication Path	Designated Storage and/or Transmission Channel
U.S. Federal Government Customer Support Requests	U.S. Federal Government Customers to HCL	HCL FSC telephone support (855) 855-5016   (984) 333-9014 HCL FSC web portal <a href="https://hclpnpsupport.hcltech.com/csm?id=federal">https://hclpnpsupport.hcltech.com/csm?id=federal</a> HCL FSC Secure Email: <a href="mailto:hclfederalsupport@hclgov.com">hclfederalsupport@hclgov.com</a> HCL FSC URL for customer facing ticketing system: <a href="https://hclpnpsupport.hcltech.com/csm?id=federal">https://hclpnpsupport.hcltech.com/csm?id=federal</a> U.S. Federal Government CuDaR: <a href="https://us-pnp-ftp03.hcl.com/">https://us-pnp-ftp03.hcl.com/</a> U.S. Federal Government CuDaR SFTP Server: 192.8.18.15
U.S. Federal Government Customer Non-Support Requests	U.S. Federal Government Customers to HCL	Email: <a href="mailto:HCLFEDERAL@immixgroup.com">HCLFEDERAL@immixgroup.com</a>
U.S. Federal Government Customer License Key Management Support Requests	U.S. Federal Government Customers to HCL	<a href="mailto:HCLSupport@vertosoft.com">HCLSupport@vertosoft.com</a> (provided by Federal Business Partner)
U.S. Federal Government Support Records	Data Storage	Federal Ticketing Backend: <a href="https://cudar-njdc.prod.hclpno.com">cudar-njdc.prod.hclpno.com</a> Federal Ticketing Transition: <a href="https://us-fedticketing.prod.hclpnp.com">us-fedticketing.prod.hclpnp.com</a> Federal CuDaR Backend: <a href="https://us-qual-lnx01.proc.hclpnp.com">us-qual-lnx01.proc.hclpnp.com</a>
U.S. Federal Government Customer Business Identifiable Information and U.S. Federal Government Customer Support Records	IBM to HCL	AWS Gov Cloud: <a href="#">hcl-awsg-dataexg account</a>
U.S. Federal Government Customer Business Identifiable Information	HCL to Federal Business Partner	AWS Gov Cloud: <a href="#">hcl-awsg-dataexg account</a>
U.S. Federal Government Customer Support Records (entitlements)	Federal Business Partner to HCL	U.S. Federal Government CuDaR SFTP Server: 192.8.18.15
HCL Federal Software Download and License Entitlement Portal	Between U.S. Federal Government Customers, HCL, and/or Federal Business Partner	<a href="https://hclgov.poetic-software.com">https://hclgov.poetic-software.com</a> (provided by Federal Business Partner)
Email containing U.S. Federal Government Customer Business Identifiable Information*	Between U.S. Federal Government Customers, HCL, IBM, and/or Federal Business Partner	@hclgov.com (Notes/Domino hosted in AWS Gov Cloud: <a href="#">hcl-awsg-mail account</a> ) @hclfederal.com (Provided by Federal Business Partner)
Notes/Domino Databases containing U.S. Federal	Data Storage	@hclgov.com (Notes/Domino hosted in AWS Gov Cloud: <a href="#">hcl-awsg-mail account</a> )


Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	<b>CFIUS Security Policies</b>	DOC.NO. CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO. 1.00 DATE 15-Jan-2020 PAGE NO. 59 of 93

Type of Request or Data	Communication Path	Designated Storage and/or Transmission Channel
Government Customer Business Identifiable Information		
U.S. Federal Government Customer Business Identifiable Information	Data Storage	End User Workstations compliant with HCL/Federal Business Partner security policies (note, documents and files may not be stored in any file sharing system, including, but not limited to, OneDrive, Microsoft Teams, Microsoft 365, or SharePoint)
U.S. Federal Government Customer Business Identifiable Information	Instant Messaging	None

\*Encrypted attachments containing U.S. Federal Government Customer Business Identifiable Information may be transmitted via @hcl.com or @pnp-hcl.com email.


	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	60 of 93

# CFIUS050

## CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment

Version 1.00

Date: 18 December 2019

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	61 of 93

## 1. Purpose

The purpose of this policy is to implement the requirements of the National Security Agreement made among HCL, International Business Machines (“IBM”), and the U.S. Government to secure and logically separate the Secure Software Build Environment (“SSBE”) and the Federal Support Environment (“FSE”) from the broader HCL network.

## 2. Scope

This policy applies to the SSBE, including the internal data center network, infrastructure, and computing assets, cloud infrastructure, and partner hosting infrastructure, as well as to the FSE, utilized in the delivery of In-Scope Software Products to U.S. Federal Government Customers.

## 3. Definitions

Capitalized terms used herein and not otherwise defined have the meaning set forth in the Glossary (CFIUS001 - Glossary of Terms Related to CFIUS Security Policies).

**“Multi-Factor Authentication”** means authentication using two or more different factors to achieve authentication. Factors include: (i) something the user knows for example, a password or personal identification number, (ii) something a user possesses such as cryptographic identification device; or (iii) something a user is, for example, a biometric.

**“Portable Computing Device”** means a general-purpose computer that (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate physically connected to external input and output devices, and (iii) does not have a self-contained power source. A Raspberry Pi is an example of a Portable Computing Device.

## 4. Policy Statements

It is the policy of HCL that:

Only Approved Personnel shall be permitted access to the SSBE and the FSE pursuant to CFIUS020 – CFIUS Access Control Policy.

The SSBE shall be logically segregated from the general HCL network through the use of firewalls and virtual local area networks (VLANs) configured consistent with this policy.

HCL shall configure elements of the SSBE and FSE to require Multi-Factor Authentication where appropriate.

HCL shall establish a change management procedure, including review and approval by an appropriate change authority, for making changes to the SSBE and the FSE.


## 5. Roles and Responsibilities

### *Information Technology Implementation Leader*

The Information Technology (IT) Implementation Leader is responsible for maintaining the design and operation of the SSBE and FSE networks in compliance with the CFIUS Security Policies. The IT Implementation Leader shall

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	62 of 93

maintain the CFIUS asset inventory and oversee the change management process for the SSBE and the FSE as the chair of the Federal Systems Change Control Task Force.

## 6. Policy Details and Corresponding Procedures

### 6.1 Overview of the Secure Software Build Environment

The SSBE is a development environment for In-Scope Software Products that is made up of multiple information systems and software applications. Some elements of the SSBE are hosted in HCL's New Jersey Data Center (NJDC), while others are hosted in cloud-based services. See Appendix A: SSBE High Level Diagram for a network diagram depicting the SSBE.

Data in the SSBE, with the exception of software Releases approved for publication in accordance with CFIUS030 – CFIUS Product Integrity Policy, is classified as HCL Confidential, as defined in the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.

### 6.2 Overview of the U.S. Federal Support Environment

The FSE is a ticketing tool and customer data repository dedicated to U.S. Federal Government Customers and accessible only to Approved Personnel. See Appendix B: FSE High Level Diagram for a network diagram depicting the FSE.

Data in the FSE is classified as HCL Confidential as defined in the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.

### 6.3 Physical Layer Controls

#### *Physical Access*

Physical Access to the SSBE and FSE shall be governed in accordance with CFIUS060 - CFIUS Physical Security Policy and CFIUS020 – CFIUS Access Control Policy.

#### *Portable Computing Devices*

No Portable Computing Devices shall be physically connected to the SSBE or FSE.

#### *Data Destruction*


Destruction of physical media shall be managed in accordance with CFIUS060 - CFIUS Physical Security Policy.

#### *Inventory of Authorized Devices and Applications*

The IT Implementation Leader shall maintain an up-to-date inventory of all authorized devices and applications comprising the SSBE, the FSE and/or otherwise containing U. S. Federal Government Customer Data in accordance with CFIUS020 – CFIUS Access Control Policy, CFIUS040 – U.S. Federal Government Customer Support and Data Protection Policy and the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.

### 6.4 Network Layer Controls

The IT Implementation Leader shall maintain up-to-date network diagrams to reflect changes in underlying architecture and production environments. Network traffic must be controlled, managed and periodically evaluated to identify vulnerabilities.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	63 of 93

### *Network Isolation Controls*

The SSBE environment shall be network segregated at the logical layer from the HCL Software information technology environment, except through specific point-to-point connections enabled through firewall configurations consistent with this policy.

### *Firewall Controls*

Firewalls protecting the SSBE network and the FSE network shall be configured in accordance with the following controls. Exceptions must be approved by the FSCC-TF.


- All firewalls and network components must be monitored to ensure they are available
- Inbound internet traffic must be protected by a physical firewall
- Firewalls must be present at any interconnection to a shared environment and/or third-party network
- Firewalls must be configured to implicitly deny inbound and outbound connections
- Firewall rules must be configured to reflect the principle of least privilege
- All firewall traffic inbound must be logged, including all administrative access
- Remote administration of the firewall from the outside interface is not permitted
- Firewall events shall be monitored for real-time security event detection
- Stateful inspection, also known as dynamic packet filtering, must be implemented
- Periodic reviews must be carried out to ensure there is a valid business reason for all services and ports open on that firewall
- All firewall rules shall have defined service/port numbers with business justification. No firewall rule shall have “ANY” as service/protocols.
- All tunnel configuration shall be followed with node communication state that should be allowed through the tunnel.
- No insecure protocols shall be permitted without a documented security exception approved by the Federal Systems Change Control Task Force (FSCC-TF). Examples of insecure protocols include FTP and telnet.
- Firewalls must be configured to prohibit SMTP email traffic unless a documented security exception is approved by the FSCC-TF
- Connectivity from the SSBE to the internal environment must be point (Source IP) to point (Destination IP) and with specific direction flow such as uni-directional or bi-directional. No broader subnets are allowed in source and destination unless an exception is granted by the change authority.
- Connectivity from the SSBE to the external (Internet) destinations must be point (Source IP) to point (Destination IP) and with specific direction flow such as uni-directional or bi-directional. No subnet ranges are allowed in source and destination unless an exception is granted by the FSCC-TF.
- Permitted ports and protocols and/or services shall be explicitly specified in the firewall’s configuration. No broader ranges of ports are allowed unless a documented security exception is approved by the FSCC-TF.

### *Virtual Local Access Network Controls*

Virtual Local Access Networks (VLANs) in the SSBE and the FSE shall be configured such that separate VLANs support the following functions: server management, console access, backup network, storage area network, and data network. Production environments must be on different VLANs from development and test environments.

### *Multi-Factor Authentication*

Access to the SSBE network in HCL’s NJDC shall require two layers of authentication with unique credentials or Multi-Factor Authentication in accordance with the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	64 of 93

### *Encryption Controls*

Encryption shall be deployed, configured, and utilized within the SSBE and the FSE in accordance with the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.

### *Network Monitoring*

Network monitoring of the SSBE and the FSE shall be conducted in accordance with the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.

## **6.5 Server Controls**

### *Access Management*

Access to servers in the SSBE and the FSE shall be restricted to Approved Personnel. Access shall be managed in accordance with CFIUS020 – CFIUS Access Control Policy.

### *Password Change Requirements*

Passwords for servers in the SSBE and the FSE shall be changed in accordance with ISMA012 – Information Security Policy.

### *Hardened System Images*

Standardized, secure OS configurations shall be developed and deployed. Unnecessary services, applications and network protocols shall be removed or disabled, in accordance with the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.

### *Malware Detection and Response*

Anti-malware software shall be deployed on servers to detect and eradicate any infections that occur, in accordance with the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products. Exceptions must be approved by the FSCC-TF.

## **6.6 Application Layer Controls**

### *Access Management*

Access to applications in the SSBE and the FSE shall be managed in accordance with CFIUS020 – CFIUS Access Control Policy and the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.

### *Multi-Factor Authentication*

Software development applications shall be integrated with Active Directory and shall be configured to require Multi-Factor Authentication in accordance with the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products. The Active Directory for the SSBE and FSE shall be segregated from the HCL corporate Active Directory.


### *Password Change Requirements*

Passwords for applications in the SSBE and the FSE shall be changed in accordance with ISMA012 – Information Security Policy.

### *Remote Access*

The provision and operation of remote access to the SSBE shall be governed by the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	65 of 93

## 6.7 Controls for Cloud Services

### *Cloud Computing Accounts*

Cloud computing services utilized in the SSBE or the FSE shall be deployed through AWS cloud services (US regions only) or AWS GovCloud (US)<sup>2</sup> accounts for Approved Personnel only. Any commercial cloud computing service used must be restricted to US regions only for storage, networking and hosting.

### *Cloud Computing Storage Services*

All cloud-based storage services shall be configured with access policies that prohibit public access to the storage location. Further, cloud-based storage services shall be configured with access policies at the user and folder levels. In both the SSBE and FSE, all data exchange storage shall be conducted using an AWS GovCloud (US) account.

### *Multi-Factor Authentication*

The identify and access management policy for all AWS and AWS GovCloud user identities shall be configured with Multi-Factor Authentication enabled.

### *Cloud-based Virtual Machines*

Internally facing cloud-based computing infrastructure, for example internally facing virtual machines deployed on Amazon Elastic Compute Cloud (EC2), shall be configured to prohibit direct access from the Internet, for example, through an EC2 Elastic IP Address. Any virtual machines which must be accessed via the Internet shall be configured behind a front-end application, such as a console. That front-end application shall be configured for authentication with user accounts and Multi-Factor Authentication. For the avoidance of doubt, this control is not required for externally facing virtual machines designed for the use of HCL Software customers.

## 6.8 Incident Response

Response to Security Incidents and Security Events inside the SSBE and the FSE shall be handled in accordance with CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers.

## 6.9 Vulnerability and Patch Management


Vulnerability and Patch Management of the SSBE and the FSE shall be conducted in accordance with the Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products.

## 6.10 Change Control

The Federal Systems Change Control Task Force (FSCC-TF) may, from time to time, modify the applications and the architecture of the SSBE and the FSE. The FSCC-TF consists of representatives from the following functions: information technology operations, information security, U.S. national security compliance, and product development. The IT Implementation Leader serves as the chair of the FSCC-TF and oversees its operation. The FSCC-TF shall exercise change management authority over the SSBE and the FSE, ensuring that approved changes are consistent with the CFIUS Security Policies.

# 7. Audit & Record-Keeping

<sup>2</sup> AWS GovCloud (US) is an isolated Amazon Web Service designed to enable users to meet specific U.S. government compliance regimes.

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	66 of 93

HCL must maintain certain records of its activities executing the policies and procedures in this document for purposes of supporting audits of its compliance with its obligations toward CFIUS. Records shall include:

- Logs – Authentication and events logs of devices and applications
- Access – Successful and unsuccessful user login attempts and privileged access attempts
- Configuration – Point in time snapshots of configuration
- Access Control List – Users lists from the device or application with privileges and roles (including both enabled and disabled)

## 7.1 Retention Policy

HCL must retain the records identified in this section for a minimum of three years. For these records, this retention period supersedes any applicable shorter retention period established in the HCL Records Retention and Destruction Policy. To the extent that the HCL Records Retention and Destruction Policy schedules require a longer period for these records, the HCL Records Retention and Destruction Policy applies.

## 7.2 Firewall Rules, Access & Logs

- Firewall rules inspection, validation and usage report on monthly basis
- Monthly access audit report
- Monthly firewall logs report on events, incidents and changes.

## 7.3 Network Switch Configuration, Access & Logs

- Network switch configuration report on monthly basis
- Monthly access audit report
- Monthly switch logs report on events, activities and changes

## 7.4 Server Access Controls & Logs

- Monthly server access log audit report
- Monthly server event and change log report

## 7.5 Storage Configuration, Access & Logs

- Monthly storage configuration report
- Monthly storage device access log report
- Monthly storage events and change log report

## 7.6 AWS Access Controls


- Monthly AWS Identity and Access Management (“IAM”) and access log report

## 7.7 Other Logs

- Core infrastructure applications access log audit report

# 8. Related Documents


The following related documents are associated with this policy:

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	67 of 93

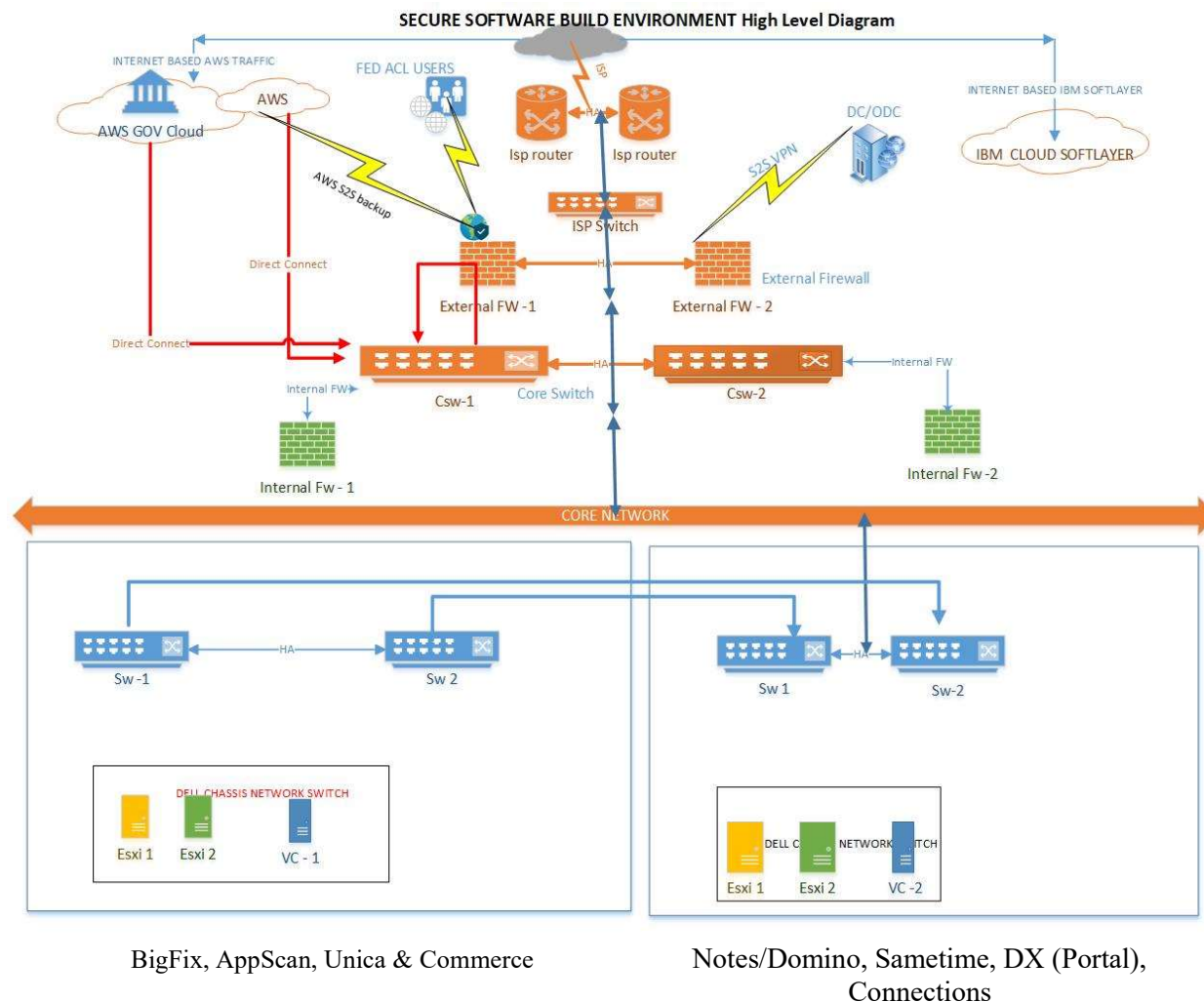
21. ISMA012 – Information Security Policy
22. HCL Records Retention and Destruction Policy
23. CFIUS001 - Glossary of Terms Related to CFIUS Security Policies
24. CFIUS020 – CFIUS Access Control Policy
25. CFIUS030 - CFIUS Product Integrity Policy
26. CFIUS040 – U.S. Federal Government Customer Support and Data Protection Policy
27. CFIUS060 - CFIUS Physical Security Policy
28. CFIUS070 - CFIUS Security Incident Response Policy for U.S. Federal Government Customers
29. Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products


## 9. Change Log

Version	Date	Author(s)	Summary of Changes
1.00	December 18, 2019	Raj Dhanawade	Final document
1.00	January 15, 2020	Karen Plonty	Approved by the CFIUS Governance Committee without changes.

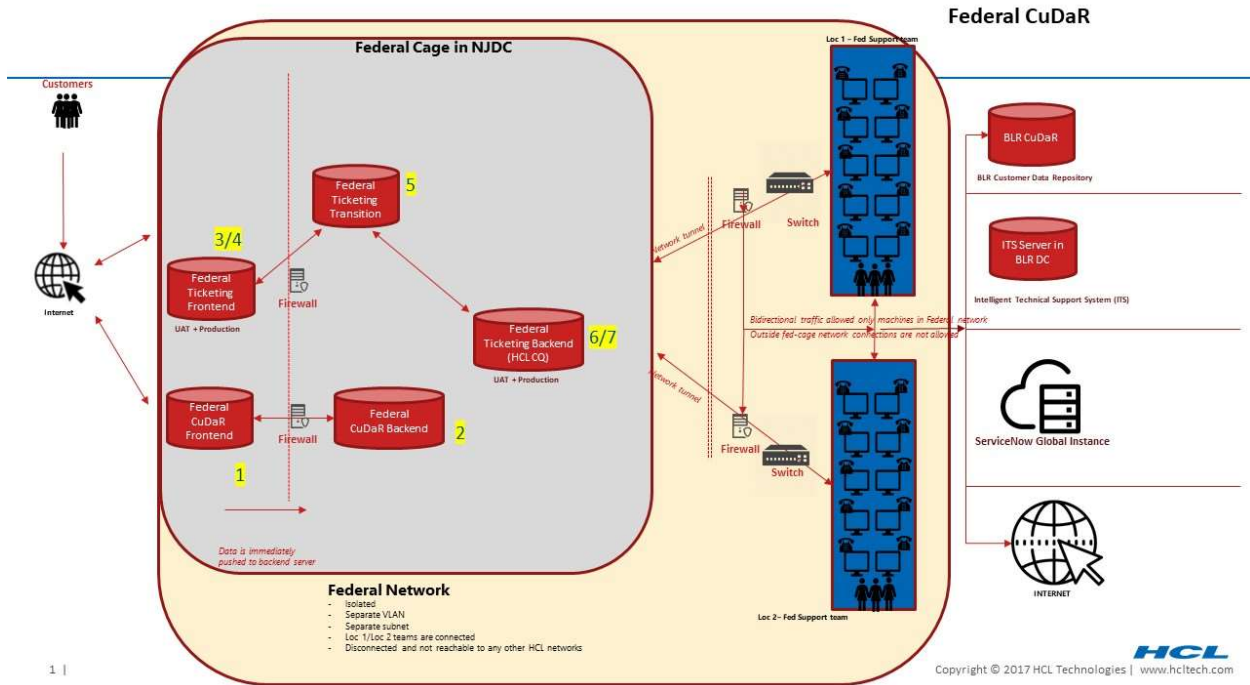
	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	68 of 93


## Appendix A: SSBE High Level Diagram



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	69 of 93

## Appendix B: FSE High Level Diagram




	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	70 of 93

# CFIUS060

## CFIUS Physical Security Policy

Version 1.00

Date: 18 December 2019

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	71 of 93

## 1. Purpose

The purpose of this document is to implement the physical security requirements of the National Security Agreement made among HCL, International Business Machines (“IBM”), and the U.S. Government.

## 2. Scope

This policy applies to all Personnel engaged in activities at any facility that is a Federal Data Center Facility or a Federal Support Room Facility.

## 3. Definitions

Capitalized terms used herein and not otherwise defined have the meaning set forth in the Glossary (CFIUS001 – Glossary of Terms Related to CFIUS Security Policies).

**“Electronic Storage Media”** means storage media including, but not restricted to, compact discs, tapes, pen drives, and cameras etc.

**“Federal Data Center Facility”** means any HCL facility that is not a Federal Support Room Facility and is primarily designed to function as a data center that houses information systems that are part of the Secure Software Build Environment (SSBE) or the Federal Support Environment (FSE).

**“Federal Support Room Facility”** means the rooms and associated data closets located in HCL facilities that are specifically configured for Approved Personnel to support U.S. Federal Government Customers.

**“Federal System Rack”** means a rack in a Federal Data Center Facility that houses information systems that are part of the SSBE or the FSE.

**“Federal System Rack Key Storage Locker”** means the uniquely-keyed storage locker that houses and secures all padlock keys used to secure Federal System Racks at Federal Data Center Facilities.


**“Visitor”** means any person requesting access to a Federal Support Room Facility or a Federal Data Center Facility who has not been authorized for unescorted access to that facility in accordance with this Policy.

## 4. Policy Statements

It is HCL’s policy that:

Physical access to any HCL building hosting a Federal Support Room Facility shall be governed by the HCL Physical Security Policy.

Physical access to any HCL building hosting a Federal Data Center Facility shall be governed by the applicable location-specific HCL security policy approved by the CFIUS Security Officer for this purpose (see HCL New Jersey Data Center Access and Security Policy).

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	72 of 93

Only Approved Personnel may be permitted physical access to any Federal System Rack with the exception of escorted Visitors authorized for such access pursuant to Section 6.1 of this policy.

All Federal System Racks shall have access restricted by padlocks or biometric locks deployed pursuant to the procedures established in this Policy.

Only Approved Personnel may be permitted physical access to any Federal Support Room Facility with the exception of escorted Visitors authorized for such access pursuant to Section 6.2 of this policy.

## 5. Roles and Responsibilities

### 5.1 CFIUS Site Security Implementation Leader

The CFIUS Site Security Implementation Leader is a CFIUS Implementation Leader as defined in CFIUS001 - Glossary of Terms Related to CFIUS Security Policies. He or she has responsibility for a specified Federal Data Center Facility. The CFIUS Site Security Implementation Leader is responsible for implementing this Policy and all other applicable site-specific aspects of the CFIUS Security Policies at that site.

The CFIUS Site Security Implementation Leaders determines which Approved Personnel are authorized for unescorted access to the server room at the Federal Data Center for which they are responsible. The CFIUS Site Security Implementation Leader is responsible for conducting a monthly reconciliation audit of Approved Personnel with badge access to the server room, and for removing access for any Personnel who are no longer Approved Personnel authorized for unescorted access. The CFIUS Site Security Implementation Leader is also responsible for auditing the log of padlock key removals, and the record of biometric lock access to ensure only Approved Personnel authorized for unescorted access have accessed those resources.

### 5.2 Federal Support Implementation Leader

The Federal Support Implementation Leader is a CFIUS Implementation Leader as defined in CFIUS001 - Glossary of Terms Related to CFIUS Security Policies. He or she has responsibility for a specified Federal Support Room Facility. The Federal Support Implementation Leader is responsible for implementing this Policy and all other applicable site-specific aspects of the CFIUS Security Policies at that site.

The Federal Support Implementation Leader determines which Approved Personnel are authorized for unescorted access to the Federal Support Room Facility for which they are responsible. The Federal Support Implementation Leader is responsible for conducting a monthly reconciliation audit of Personnel with badge access to the Federal Support Room Facility, and for removing access for any Personnel who are no longer Approved Personnel authorized for unescorted access. The Federal Support Implementation Leader is also responsible for auditing badge access records for the Federal Support Room Facilities to ensure that only Approved Personnel authorized for unescorted access have accessed the rooms via badge reader access.


## 6. Policy Details and Procedures

### 6.1 Federal Data Center Facilities

#### *Access to the Server Room*

Federal Data Center Facilities may be in commercial data center facilities where other customers of the data center facility may obtain access to the data center's server room following the policies and procedures of the commercial data center operator.



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	73 of 93

### *Unescorted Access*

The CFIUS Site Security Implementation Leader may authorize Approved Personnel for unescorted physical access to the server room at a Federal Data Center Facility and to Federal System Racks whenever such Approved Personnel's typical job function requires it. Prior to authorizing such unescorted access, the CFIUS Site Security Implementation Leader shall validate that person's authorization on the Federal Access Control List. The CFIUS Site Security Implementation Leader shall maintain a current list of Approved Personnel granted unescorted access. A duplicate of such list shall be attached to the Federal System Rack Key Storage Locker.

The access controls established in the HCL New Jersey Data Center Access and Security Policy, or other similar location-specific policy established in accordance with Section 71 of this document, shall apply to Approved Personnel with unescorted access.

### *Visitors*

HCL may allow Visitors to access Federal Data Center Facilities, server rooms inside Federal Data Center Facilities, and Federal System Racks to service or maintain equipment and systems of the Federal Data Center Facility or to fulfill a requirement of law, regulation, or the Agreement. All such Visitors shall be subject to the following controls:

- All Visitors shall be subject to the relevant sections of the applicable location-specific HCL Security Policy (see HCL New Jersey Data Center Access and Security Policy).
- Any Visitor whose purpose for entering the Federal Data Center Facility requires access to a Federal System Rack shall have a valid service or support ticket or be approved in writing by the CFIUS Site Security Implementation Leader.
- Any Visitor whose purpose for entering the Federal Data Center Facility requires access to a Federal System Rack shall be escorted and monitored at all times within the Federal Data Center Facility by Approved Personnel authorized for unescorted access to the Federal Data Center facility.
- Visitors who require access to a Federal System Rack shall be escorted and monitored at all times by Approved Personnel to ensure they do not access U.S. Federal Government Customer Data while servicing or maintaining the equipment and systems.

### *Government Officials*

Government officials are Visitors who are duly authorized representatives of a federal, state, or local government. Examples of such government officials include, but are not limited to, law enforcement officials, tax officials, and fire officials. Any Personnel who become aware of request to enter the Federal Data Center Facility from a government official, whether previously notified to HCL or not, shall immediately notify the responsible CFIUS Site Security Implementation Leader and the CFIUS Security Officer.

In the case of a visit by a government official representing the CFIUS Monitoring Agencies, the relevant sections of CFIUS010 – CFIUS Governance, Oversight and Notification Policy apply.


### *Procedures for Deploying Padlocks on Federal System Racks*

Whenever padlocks are used to restrict access to Federal System Racks, padlocks shall be deployed in conjunction with a heavy-duty chain that prevents the rack from opening while the padlock is locked. To the extent possible given the physical design of a given rack, padlocks and chains shall be deployed according to the following procedure:

- Secure both the front and rear access door to each rack, using separate chains and padlocks for each side of the rack. Use a pair of padlocks that are keyed identically such that the same key opens both the front and rear padlocks.
- Ensure that the keys are numbered, the padlocks are numbered, and that the numbers match.
- Ensure that one and only one rack is secured by a pair of padlocks that open with a given key. No key may open more than one rack.

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	74 of 93

- Pass the chain through the small opening in each door near the top of the door on the same side as the handle, to the inside of the rack.
- Pass the chain through the top of the rack. Loop the chain around to the outside of the door.
- Join the chain on the outside of the rack with a padlock, passing the lock's shackle through links on each end
- Ensure that the movement of the chain through the door is restricted.

### *Opening and Closing Padlocked Federal System Racks*

Whenever a Federal System Rack is unlocked, Approved Personal authorized for unescorted access in possession of the padlock key to that open Federal System Rack shall remain physically at the rack. The person who unlocked the padlock is solely responsible for securing the chain and locking the padlock, following the procedures in this section, whenever Approved Personal authorized for unescorted access in possession of the padlock key are not at the rack.

At the end of each business day, Approved Personnel shall inspect each Federal System Rack secured by padlock to verify that the rack is properly secured.

### *Procedures for Padlock Key Management*

All keys for the padlocks securing Federal System Racks shall be stored in a Federal System Rack Key Storage Locker when not in the immediate personal possession of Approved Personnel authorized for unescorted access. No other keys shall be stored in the Federal System Rack Key Storage Locker. No key to any padlock used to restrict access to a Federal System Rack may be removed from the Federal Data Center Facility.

The Federal System Rack Key Storage Locker shall be under the control of the data center operations team at the Federal Data Center Facility. Although not Approved Personnel themselves, data center operations team Personnel shall sign an acknowledgement that they will only allow Approved Personnel authorized for unescorted access to take possession of padlock keys and to unlock the Federal System Racks.

The Federal System Rack Key Storage Locker shall be physically maintained within a room at the Federal Data Center Facility that is designated for security functions, secured by a badge reader security authorization system deployed on by a server located at the data center, and overseen by the data center operations team.

The room designated for security functions may conjoined with data center room designated for other purposes, for example, a network operations center, so long as the conjoined room is also secured by a badge reader security authorization system deployed on by a server located at the data center, and overseen by the data center operations team.


Data center operations team Personnel overseeing the room designated for security functions shall verify that the valid, HCL-issued identification card of any Personnel requesting a padlock key from the Federal System Rack Key Storage Locker exactly matches an entry on the list of Approved Personnel authorized for unescorted access, prior to opening the Federal System Rack Key Storage Locker.

Whenever Approved Personnel authorized for unescorted access remove padlock keys from the Federal System Rack Key Storage Locker, that removal shall be documented on a log maintained inside the Federal System Rack Key Storage Locker by the data center operations team, in accordance with the following procedures:

- The data center operations team member who opens the Federal System Rack Key Storage Locker shall be responsible for updating the log with the following information:
  - The date and time of the key removal and return.
  - The key number removed.
  - The name of the Approved Personnel taking possession of the key
  - The purpose for Federal System Rack access.

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	75 of 93

- The signatures of the Approved Personnel and the data center operations team member when the key is removed and returned
- Both Approved Personnel authorized for unescorted access taking possession of the key and the operations team member who opened the Federal System Rack Key Storage Locker shall sign the log when the key is removed.
- The Approved Personnel authorized for unescorted access taking possession of the key shall return the key prior to the end of the same workday.
- Whenever a key is returned to the Federal System Rack Key Storage Locker, the date and time of return shall be noted in the log.
- Both the Approved Personnel authorized for unescorted access returning the key and the operations team member who opens the Federal System Rack Key Storage Locker for the key's return shall sign the log when the key is returned.

### *Procedures for Managing Master Keys for the Federal System Rack Key Storage Locker*

The Federal Data Center Facility shall maintain two (2) individually tagged and identified master keys that can individually open the Federal System Rack Key Storage Locker, and only that locker. The first master key shall be maintained by the data center operations team, within their own sign-out key locker in the data center security office. The second master key is maintained individually by a systems administrator who is onsite at the Federal Data Center Facility and who is authorized on the Federal Access Control List.

### *Procedures for Managing Biometric Locks on Federal System Racks*

Whenever a biometric lock is used to restrict access to a Federal System Rack, those biometric locks shall be configured and managed in accordance with the following controls:

- Biometric locks shall be configured to unlock only for Approved Personnel authorized for unescorted access.
- All Biometric locks shall be monitored by the console application for the locks.
- Alerts for the biometric lock shall be set to notify data center staff by email and generate a console warning if an unauthorized entry is attempted.
- Alerts for the biometric locks shall be configured to notify data center staff if the Federal System Rack it secures is open for a length of time exceeding ten (10) minutes.
- The console for the biometric locks shall be located in the Federal Data Center Facilities network operations center.


### *Opening and Closing a Biometric-Secured Federal System Rack*

Whenever Approved Personnel authorized for unescorted access unlocks a biometric lock securing a Federal System Rack, the person who unlocked the rack shall remain physically at the rack while the rack is open. The person who unlocked the biometric lock is solely responsible for securing the rack if that person leaves the rack for any reason.

## **6.2 Federal Support Room Facilities**

### *Unescorted Access*

The Federal Support Implementation Leader may authorize Approved Personnel for unescorted physical access to the Federal Support Room Facility (including associated data closets) whenever such Approved Personnel's typical job function requires such access. Prior to authorizing unescorted access for any person, the CFIUS Site Security Implementation Leader shall validate that person's authorization on the Federal Access Control List.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	76 of 93

The Federal Support Room Facility doors shall be secured by a badge reader security authorization system. That badge reader security authorization system shall be configured to allow access to the Federal Support Room Facility only to Approved Personnel authorized for unescorted access.

### *Visitors*

HCL may allow Visitors to access Federal Support Room Facilities to service or maintain equipment and systems of the Federal Support Room Facilities or to fulfill a requirement of law, regulation, or the Agreement. All such Visitors shall be subject to the following controls:

- All Visitors shall be subject to the relevant sections of the HCL Physical Security Policy.
- Any Visitor to a Federal Support Room Facility shall be approved in writing by the Federal Support Implementation Leader prior to entering the Federal Support Room Facility.
- Any Visitor to a Federal Support Room Facility shall be escorted and monitored at all times by Approved Personnel to ensure they do not access U.S. Federal Government Customer Data.
- Any Visitor to a Federal Support Room Facility shall provide a valid HCL-issued or government-issued identification to the Federal Support Implementation Leader or his or her designee for purposed of recording the visit in a written log prior to entering the Federal Support Room Facility.

### *Government Officials*

Any Personnel who become aware of request to enter the Federal Support Room Facility from a government official, whether previously notified to HCL or not, shall immediately notify the cognizant Federal Support Implementation Leader and the CFIUS Security Officer.

In the case of a visit by a government official representing the CFIUS Monitoring Agencies, the relevant sections of CFIUS010 – CFIUS Governance, Oversight and Notification Policy apply.

## **6.3 Third Party Monitor and Third-Party Auditor Inspection**

To facilitate the performance of the duties assigned to the Third-Party Monitor and the Third-Party Auditor as described in CFIUS010 – CFIUS Governance, Oversight, and Notification Policy, HCL shall grant the Third-Party Monitor and the Third-Party Auditor, upon reasonable prior notice and during normal business hours, escorted access to all Federal Data Center Facilities and Federal Support Room Facilities.


## **6.4 Asset Disposal and Data Destruction**

Any electronic media used in the Secure Software Build Environment or the U.S. Federal Support Environment physically located in a Federal Data Center Facility or a Federal Support Room Facility shall not be removed from that facility without first undergoing media sanitization consistent with National Institutes of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization. Exceptions require written approval from the CFIUS Security Officer.

Any media that cannot be sanitized pursuant to the above noted NIST standard shall be physically destroyed. A written log of any media destruction shall be maintained at each Federal Data Center Facility and each Federal Support Room Facility. The log shall contain an attestation regarding each destruction from no less than two Approved Personnel.

## **6.5 Personal Electronic Storage Media**

The introduction of any personal Electronic Storage Media of any type (e.g., USB drives) to a Federal Data Center Facility or a Federal Support Room Facility is prohibited per the HCL Physical Security Policy.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	77 of 93

## 7. Audit & Record-Keeping

### 7.1 Badge Reader Access Records

All Federal Data Center Facilities and the Federal Support Room Facilities shall implement procedures to document and maintain badge reader access records. The records shall be made available to the CFIUS Security Officer or their designee upon request. For details, refer to the HCL Physical Security Policy.

### 7.2 Visitor Logs

All Federal Data Center Facilities and the Federal Support Room Facilities shall implement procedures to document and maintain visitor logs. The records shall be made available to the CFIUS Security Officer or their designee upon request. For details, refer to the HCL Physical Security Policy.

### 7.3 Key Control Logs

All Federal Data Center Facilities shall implement procedures to document and maintain key control logs. The records will be made available to the CFIUS Security Officer or their designee upon request.


## 8. Related Documents

The following related documents are associated with this policy:

1. [HCL Physical Security Policy](#)
2. HCL New Jersey Data Center Access and Security Policy
3. CFIUS001 - Glossary of Terms Related to CFIUS Security Policies
4. CFIUS010 – CFIUS Governance, Oversight, and Notification Policy
5. CFIUS020 - CFIUS Access Control Policy

## 9. Change Log

Version	Date	Author(s)	Summary of Changes
1.00	December 18, 2019	James Flenniken	Final document
1.00	January 15, 2020	Karen Plonty	Approved by the CFIUS Governance Committee without changes.


	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	78 of 93

# CFIUS070

## CFIUS Security Incident Response Policy for U.S. Federal Government Customers

Version 1.00

Date: 18 December 2019

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	79 of 93

## 1. Purpose

The purpose of this Incident Response Policy (IRP) is to implement the incident response requirements of the National Security Agreement made among HCL, International Business Machines (“IBM”), and the U.S. Government.

This IRP provides the consistent framework for HCL to respond to a Security Incident impacting the Secure Software Build Environment, the Federal Support Environment and the availability, confidentiality, and integrity of the U.S. Federal Government Customer Data. This IRP provides high level guidance to prevent the loss of information, property, and reputation in the event of a Security Incident. Additionally, this IRP provides a documented methodology for identifying, reporting and responding to such incidents and is aligned with HCL’s corporate security incident response plan (see ISMG019 – Information Security Incident Response Plan).

This document will serve as a guide to facilitate a response in a systematic manner to Security Incidents and is designed to (a) prevent or minimize disruption of critical information systems; (b) minimize loss or theft of sensitive or critical information; and (c) quickly and efficiently remediate and recover from Security Incidents. In accordance with the confidential National Security Agreement (the “Agreement”) made between HCL, IBM, and the U.S. Government, this IRP has been designed using National Institutes of Standards and Technology (NIST) [Special Publication 800-61](#), “Computer Security Incident Handling Guide.”

## 2. Scope

All HCL Personnel are required to promptly report Security Incidents according to the procedures described in this IRP. All other aspects of this IRP are applicable to all HCL Personnel engaged in activities involving the Source Code Development Process for In-Scope Software Products, the Secure Software Build Environment, the Federal Support Environment and U.S. Federal Government Customer Data.

This IRP covers the Secure Software Build Environment, Federal Support Environment and U.S. Federal Government Customer Data consistent with the scoping statement of ISMG019 – Information Security Incident Response Plan: “... engagements with specific contractual obligations or other established requirements specific to the customer and related to Security Incident Management will be governed by process and procedures established at the customer engagement level.” This IRP covers Security Incidents involving In-Scope Software Products, U.S. Federal Government Customer Data, Source Code for the In-Scope Software Products, the Secure Software Build Environment and the Federal Support Environment.

Security Incidents include, but are not limited to:


- Any suspected vulnerability in the In-Scope Software Products
- Any suspected unauthorized access to the Secure Software Build Environment or Federal Support Environment
- Any suspected unauthorized access to or disclosure of U.S. Federal Government Customer Data
- Any suspected compromise or unauthorized change to HCL product code regardless of whether the code was introduced into the Secure Software Build Environment or not

HCL Personnel are required to promptly report all Suspected Breaches of this policy to the Security Implementation Leader.

## 3. Definitions

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	80 of 93


Defined below are terms specific to this IRP. Capitalized terms used herein and not otherwise defined have the meaning set forth in CFIUS001 – Glossary of Terms Related to CFIUS Security Policies.

**“Incident Record”** means a record of a reported Security Incident, including a Product Security Vulnerability” that is created, tracked, and updated by the IRT until it is resolved.

## 4. Policy Statement

HCL will maintain and follow a documented incident response program consistent with NIST guidelines for computer security incident handling regarding In-Scope Software Products delivered to U.S. Federal Government Customers.



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	81 of 93

## 5. Roles and Responsibilities

Roles and responsibilities for incident response include but may not be limited to those in Table 1. These roles are not intended to match any specific person's formal job function or title but may be performed by a variety of personnel depending on the facts of the Security Incident. Further, several roles may be performed by the same individual.

*Table 1- Roles and Responsibilities*

Title	Role & Responsibilities
<b>Incident Reporter</b>	Incident Reporters who are U.S. Federal Government Customers report potential Security Incidents to the HCL Federal Support Center (see CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy). Incident Reporters who are HCL Personnel report potential product vulnerabilities via the PSIRT reporting tool ( <a href="mailto:psirt@hcl.com">psirt@hcl.com</a> ). All other suspected incidents are reported to the HCL Software Information Security & Compliance team. The Incident Reporter provides all requested information when reporting a potential Security Incident and while engaged by the appropriate Incident Response Team. HCL Incident Reporters will be available to work with the HCL CSIRT or PSIRT until no longer required, including participating in lessons learned meetings, if required.
<b>Incident Response Team</b>	<p>The Incident Response Team (IRT) is responsible for determining the nature of the event and determining if an actual Security Incident has occurred. This team will be responsible for the initial risk assessment and declaration of a Security Incident to the Security Implementation Leader. The specific skill sets needed on this team will vary based on the nature of the Security Incident. Members may include the Security team lead, product-specific security focal points, federal helpdesk and system administrators.</p> <p>For product-related Security Incidents, including Product Security Vulnerabilities, the IRT is referred to as the Product Security Incident Response Team (PSIRT). For all other non-product-related Security Incidents, the IRT is referred to as the Computer Security Incident Response Team (CSIRT).</p>
<b>Managing Counsel</b>	The role of Managing Counsel is to provide advice as needed in connection with a Security Incident. This can include ensuring the protection of privilege, the legal usability of evidence collected, and handling any potential liability issues. Managing Counsel can utilize supplemental external resources as necessary should the need arise.
<b>PSIRT Program Manager</b>	The PSIRT Program Manager manages the Product Security Incident Response Team workflow under the direction of the Security Implementation Leader.
<b>Security Implementation Leader</b>	The Security Implementation Leader is responsible for implementing and overseeing execution of this IRP. The Security Implementation Leader conducts a preliminary investigation of all reported Security Incidents and notifies the CFIUS Security Officer of all Security Incidents that either constitute a Suspected Breach or require further review.
<b>CFIUS Security Officer</b>	The CFIUS Security Officer investigates reported Suspected Breaches arising from Security Incidents and determines whether such breaches shall be deemed Known Breaches as described in CFIUS010 – CFIUS Governance, Oversight and Notification Policy.

<b>HCL</b>	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	82 of 93

## 6. Policy Details and Corresponding Procedures

HCL will execute the following workflow for all Security Incidents:

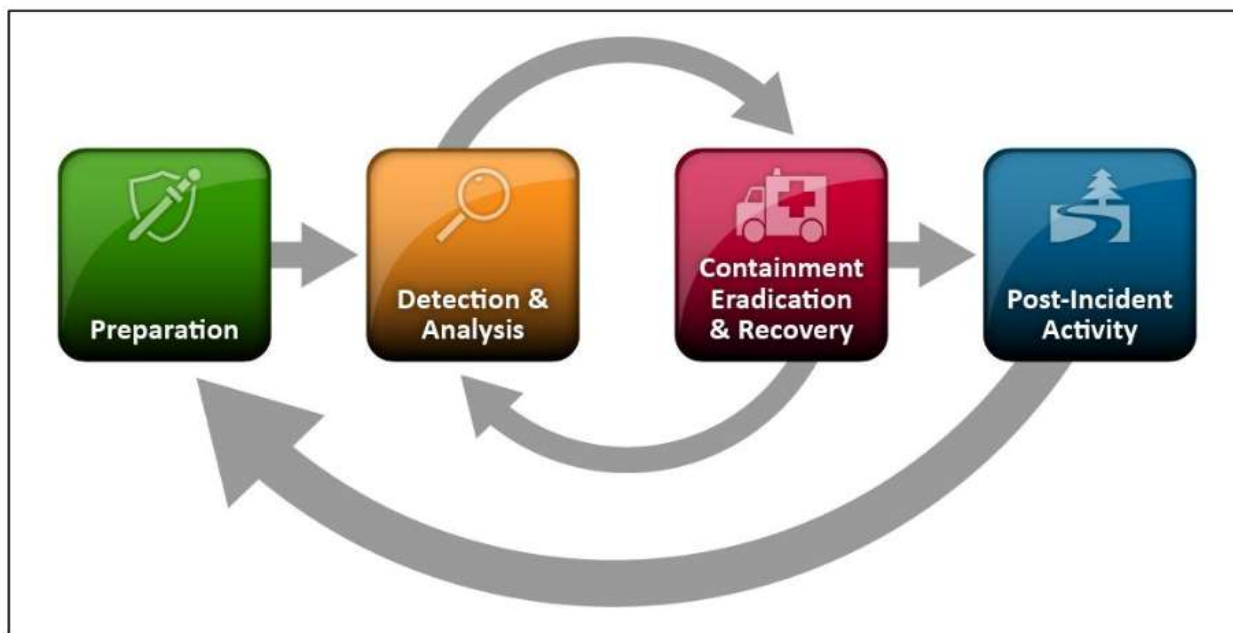


Figure 1- Incident Response Life Cycle from NIST SP800-61r2


The steps executed during the workflow will vary depending on the type of incident that is being investigated. The main types of Security Incidents include:

- Actual Security Vulnerabilities involving In-Scope Software Product Security Vulnerabilities (“Product Security Vulnerabilities”)
- A single or series of security events with negative consequences in an information system or network that (i) involve unauthorized access, use, disclosure, disruption, modification, or destruction of HCL’s information systems or information residing therein, (ii) have a significant adverse impact on business operations, or (iii) otherwise violate or present an imminent threat of violation of HCL’s information security policies, acceptable usage policies or standard security practices.

### 6.1 Preparation

HCL will maintain the security protections outlined in the CFIUS050 – CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment. These include, but are not limited to, network isolation controls, firewalls, access management, malware detection and response, and vulnerability and patch management. Training on CFIUS Security Policies will be given to all HCL Personnel who perform services relating to In-Scope Software Products delivered to U.S. Federal Government Customers, as described in CFIUS010 – CFIUS Governance, Oversight and Notification Policy. Training will be commensurate to the job functions and duties of each group.

For product-related Security Incidents, including Product Security Vulnerabilities, the PSIRT Program Manager will train all Personnel involved in the end-to-end PSIRT workflow on the requirements that must be met, from receiving initial notification of Product Security Vulnerabilities through to resolution and communication to customers. The

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	83 of 93

PSIRT Program Manager will ensure that all Personnel who have a part to play in the PSIRT workflow have been informed and are prepared to take appropriate action regarding Product Security Vulnerabilities to prevent potential Security Incidents, as well as actual Security Incidents.

The Security Implementation Leader will validate that all applicable people in their respective organizations have been trained on the availability and appropriate use of security tools and monitoring services.


## 6.2 Detection & Analysis

Security Incidents for In-Scope Software Products can result from Product Security Vulnerabilities detected by security software scans, security researchers and customers, as well as through malware and other attack vectors from outside the secure environment. The HCL Software Information Security & Compliance Team shall review security logs of activity in both the Secure Software Build Environment and the Federal Support Environment to identify potential Security Incidents. The CFIUS Implementation Leader, PSIRT Program Manager or other product security focal point will work with Incident Reporters to ensure that sufficient details are provided to identify the nature and possible source of the Security Incident.

Potential Security Incidents may be reported by internal or external sources. These include, but are not limited to, U.S. Federal Government Customers, HCL Personnel and third-party monitoring agencies. U.S. Federal Government Customers can report a Security Vulnerability found in an In-Scope Software Product by calling the Federal Support Center. The Federal Support Center will notify the relevant PSIRT and Security Implementation Leader as described in CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy. HCL Personnel and third-parties can report a Security Vulnerability found in an In-Scope Software Product to [psirt@hcl.com](mailto:psirt@hcl.com).

Potential Security Incidents that are detected in the Secure Software Build Environment or Federal Support Environment, or that involve U.S. Federal Government Customer Data, must be promptly reported to the Security Implementation Leader. All reported potential Security Incidents will be tracked in an Incident Record database. The Security Implementation Leader, in consultation with the CFIUS Security Officer, will review all reported potential Security Incidents to determine if access to the data or systems involved must be restricted to Approved Personnel. If so, the IRT will be comprised of Approved Personnel as required. If the data or systems involved are not restricted to Approved Personnel, the Security Incident will be handled following the HCL process outlined in ISMG019 – Information Security Incident Response Plan, using the full resources of HCL as needed. The Security Implementation Leader shall conduct a preliminary investigation to determine whether the reported potential Security Incident constitutes a Suspected Breach or requires further investigation, as described below. The Security Implementation Leader shall keep detailed records of which reported potential Security Incidents are not reported to the CFIUS Security Officer and why.

When HCL receives a report of a potential product-related Security Incident for an In-Scope Software Product, it is immediately routed to the appropriate product team for analysis. The team determines if the reported Security Incident constitutes an actual Security Incident for an In-Scope Software Product, and if so, conducts a preliminary investigation, including the potential impact the Security Incident could have on U.S. Federal Government Customers. For a product-related Security Incident, including a Product Security Vulnerability, that constitutes a Suspected Breach or requires further investigation, the Security Implementation Leader will promptly forward the Security Incident report to CFIUS Security Officer, including the results of the preliminary investigation, and will keep the CFIUS Security Officer informed of all status updates to the Incident Record. For the purposes of this Policy, the Security Implementation Leader shall consider all potential Security Incidents reported by U.S. Federal Government Customers to be Suspected Breaches and shall promptly forward the Security Incident reports to the CFIUS Security Officer as described in the preceding sentence. The CFIUS Security Officer shall determine if the Suspected Breach constitutes a Known Breach and, if so, shall notify the Third-Party Monitor and the CFIUS Monitoring Agencies as required in CFIUS010 – CFIUS Governance, Oversight and Notification Policy.

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	84 of 93

When a report of a data-related or other non-product-related Security Incident is received by the Security Implementation Leader, he or she will convene an appropriate CSIRT depending on the nature and priority of such incident, including preliminary awareness to the CFIUS Security Officer. The Security Implementation Leader is responsible for determining if the reported Security Incident constitutes a Suspected Breach or requires further review. If so, he or she will promptly forward the Security Incident report and results of the preliminary investigation to the HCL CFIUS Security Officer pursuant to CFIUS010 – CFIUS Governance, Oversight and Notification Policy. The CFIUS Security Officer shall determine if the Suspected Breach constitutes a Known Breach and, if so, shall notify the Third-Party Monitor and the CFIUS Monitoring Agencies as required in CFIUS010 – CFIUS Governance, Oversight and Notification Policy.

For non-product-related Security Incidents, the CFIUS Security Officer will determine the appropriate communications that are needed to U.S. Federal Government Customers, depending on the impacted parties. Actual communications with the U.S. Federal Government Customer related to Security Incidents involving U.S. Federal Government Customer Data will be overseen by the CFIUS Security Officer in accordance with the CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy. Non-product-related Security Incidents that do not involve U.S. Federal Government Customer Data will follow the HCL process outlined in ISMG019 – Information Security Incident Response Plan, using the full resources of HCL as needed.

### 6.3 Containment, Eradication and Recovery


Product Security Vulnerabilities in general do not require any special steps for containment or recovery. The PSIRT responses to Product Security Vulnerabilities must meet HCL Software’s committed response times guidelines. Allowable response times are calculated based on the potential impact if the vulnerability is exploited and the type of software product. The potential for exploiting the vulnerability is contained when the resolution is published, and any code updates are made available through normal channels. The U.S. Federal Government Customers own the responsibility to deploy the updates on their systems to eradicate the vulnerability. The resolution will be described in a published security bulletin made available from the [Knowledge Base on the HCL Support Portal](#). If the resolution involves a Release or Test Fix, U.S. Federal Government Customers will be directed to the download location by the Federal Customer Service team. The PSIRT Program Manager will notify the Federal Support Center of any In-Scope Software Product updates that include fixes to vulnerabilities.

Other Security Incidents require a more complex response. The CSIRT will act immediately upon being notified of an incident to contain the affected resource(s). Containment actions will depend upon the nature of the incident and can include, but are not limited to, turning off access permissions, isolating a machine from the network or restricting services. Any records related to the Security Incident will be attached to the Incident Record for legal, audit and tracking purposes. A detailed log must be kept for all evidence, including the following:

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
- Security tool version
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Locations where the evidence was stored.

Eradication and Recovery are also incident-dependent. The CSIRT members will work with appropriate teams such as IT Operations, Human Resources, the Federal Support Center, and product development teams to resolve Security Incidents. All steps taken during Eradication and Recovery phases will be documented in the Incident Record.

After an incident has been contained, eradication may be necessary to eliminate components of the Security Incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the

	<b>CFIUS Security Policies</b>	DOC.NO. CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO. 1.00 DATE 15-Jan-2020 PAGE NO. 85 of 93

organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

In recovery, the CSIRT will work with IT administrators to restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists). Higher levels of system logging or network monitoring or additional user training are often part of the recovery process.

If U.S. Federal Government Customers are impacted, the CSIRT will work through the CFIUS Security Officer to assist the customer in any recovery and verification efforts. If a product update is required, the availability of the update will be made known to the Federal Support Center and the CFIUS Security Officer for communication to the affected customers, so that they can install such update to secure their systems.

The Security Implementation Leader and CFIUS Security Officer will work with the CSIRT and Managing Counsel, as needed, to ensure that the cause of the incident has been resolved, and that the Secure Software Build Environment, Federal Support Environment, and/or impacted U.S. Federal Government Customers are fully operational for any impacted In-Scope Software Product. The CFIUS Security Officer will notify the CFIUS Monitoring Agencies in accordance with the CFIUS010 – CFIUS Governance, Oversight and Notification Policy.

## 6.4 Lessons Learned

HCL collects data on many aspects of reported Security Incidents, and the HCL Software Information Security & Compliance team with the product teams will regularly analyze the data for patterns and trends and make recommendations for any additional procedures, scans or other actions to reduce future occurrences of similar incidents. The team will also use this data as an input to the Risk Assessment process. The PSIRT Program Manager holds open forum meetings with the product-specific IRTs, and encourages information sharing on issues and lessons learned regarding vulnerabilities.

## 7. Audit & Record-Keeping

All records related to any Product Security Vulnerability or Security Incident will be maintained in the appropriate Incident Record database for a minimum of 3 years. This includes any communications, system logs or similar files, which will be stored as related files to the Incident Record.

Product Security Vulnerabilities – The PSIRT Program Manager will maintain the Incident Record database for all reported product-related Security Incidents, including Product Security Vulnerabilities.

Non-product-related Security Incidents – The Security Implementation Leader will maintain the Incident Record database for all reported non-product-related Security Incidents as described in Section 6.3. Records shall include documentation of which reported Security Incidents are not reported to the CFIUS Security Officer and why.


## 8. Related Documents

The following related documents are associated with this policy:

1. ISMG019 – Information Security Incident Response Plan
2. CFIUS001 - Glossary of Terms Related to CFIUS Security Policies
3. CFIUS010 – CFIUS Governance, Oversight and Notification Policy
4. CFIUS020 – CFIUS Access Control Policy

Classification – Internal


Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	86 of 93

5. CFIUS030 - CFIUS Product Integrity Policy
6. CFIUS040 - CFIUS U.S. Federal Government Customer Support and Data Protection Policy
7. CFIUS050 - CFIUS Security Policy for the Secure Software Build Environment and Federal Support Environment
8. CFIUS060 - CFIUS Physical Security Policy
9. CFIUS080 - CFIUS Background Verification Policy
10. Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment for In-Scope Software Products

## 9. Change Log

Version	Date	Created/Modified by	List of Changes
1.00	December 18, 2019	Gail Tenney	Final document
1.00	January 15, 2020	Karen Plonty	Approved by the CFIUS Governance Committee without changes.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	87 of 93


# CFIUS080

## CFIUS Background Verification Policy

Version 1.00

Date: 18 December 2019



	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	88 of 93

## 1. Purpose

The purpose of this document is to implement the background verification requirements of the National Security Agreement made among HCL, International Business Machines (“IBM”), and the U.S. Government.

## 2. Scope

The Policy is applicable to existing HCL Personnel who are on the Federal Access Control List (“FACL”) or whose job function requires approval on the FACL.

The Policy is also applicable to all HCL Software U.S. job applicants to whom an offer of employment (permanent, fixed term, part time) has been made by HCL (“Prospective Employees”).

## 3. Definitions

Capitalized terms used herein and not otherwise defined have the meaning set forth in the Glossary (CFIUS001- Glossary of Terms Related to CFIUS Security Policies).

“**Prospective Employee**” means any HCL Software U.S. job applicant to whom an offer of employment (permanent, fixed term, part time) has been made by HCL.

## 4. Policy Statements

It is the policy of HCL that:

Personnel whose job function requires approval on the FACL must go through a background check pursuant to the requirements of the CFIUS020 – CFIUS Access Control Policy.


In addition to requirements for FACL approval, anyone who needs access to HCL systems and data over an extended period of time will go through a background check, in addition to Employees as a condition of employment. Depending on requirements of the position / client requirement, an applicant’s information will be reviewed and verified against set criteria to determine eligibility.

All Prospective Employees and existing Personnel consent to undertake background verification, and in this regard, will be required to execute requisite authorizations for allowing HCL to conduct employment background verification checks.

HCL complies with all applicable federal, state and local laws regarding execution and retention of background checks.

Existing Personnel will be required to go through a background check and the same standards outlined in this Policy must be met for continued employment with HCL. All existing Personnel must provide requisite information and documents to conduct background verification, as and when requested by HCL, in a timely manner, to enable HCL to complete the background verification process. Failure or refusal to provide requisite information in a timely manner will be treated as failure to meet the background check standards.



	<b>CFIUS Security Policies</b>	DOC.NO.	CFIUS100
	<b>U.S. National Security Compliance</b>	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	89 of 93

Circumstances that might necessitate a background check be completed on existing Personnel include, but are not limited to, new client requirements, transferring to a client team that requires a more extensive background check, being on a team that implements expanded background check or at the request of the business for other purposes.

HCL reserves the right to conduct a background check on existing Personnel at any time.

If a Prospective Employee fails to submit any document required for conducting background verification, they will not be considered for hiring.

If the results of a Prospective Employee's background verification are adverse or cannot be verified, appropriate actions including withdrawal of offer of employment will be taken based on the recommendations given by the background verification team and in line with HCL policies.

The company reserves the right to have the background checks conducted by an outside agency in accordance with applicable laws.

## 5. Roles and Responsibilities

HCL Human Resources ("HR") is responsible for initiating background verification with the background check vendor or vendors.

The background check vendor is responsible for completing the background checks within the timeframe specified in their Service Level Agreement ("SLA"), and for complying with applicable federal, state and local laws.

The HCL Background Verification ("BGV") team is a central organization within Human Resources responsible for executing the background check procedure with the background check vendor. The BGV team reviews background check results and refers concerns and discrepancies to the BGV Council. The BGV team is also responsible for maintaining background check records in accordance with applicable law and the retention policies described in this document.

The BGV Council reviews and adjudicates concerns and discrepancies in background check results.


The CFIUS Security Officer is the final decision maker for BGV adjudication decisions related to eligibility for the FACL.

## 6. Procedures

### 6.1 Background Check Procedure

The background check procedure consists of the following steps:

1. HCL Human Resources initiates background checks with the appropriate vendor or vendors that HCL has engaged for this purpose.
2. The background check vendor or vendors complete the appropriate component checks as described in this methodology within the timeframe specified in their respective Service Level Agreements. All background checks and pre-employment screens are conducted in compliance with applicable federal, state, and local laws.
3. The HCL Background Verification team reviews and dispositions background check results and refers any concerns/discrepancies to the HCL BGV Council for adjudication (see Section 6.6).

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	90 of 93

## 6.2 Incremental Background Check

HCL will conduct an incremental background check on all existing U.S. Personnel on the Federal Access Control List who require a background check pursuant to CFIUS020 – CFIUS Access Control Policy and who have previously gone through a standard background check pursuant to the corporate HCL Background Verification Policy. The incremental background check will consist of the component checks listed in Table 1. HCL will complete and adjudicate all incremental background checks for existing U.S. Personnel within 60 calendar days of the CFIUS Monitoring Agencies' concurrence with HCL's background verification methodology.

**Table 1: Component Checks for Existing U.S. Personnel**


Criminal Search to include County, State and Federal Records for past 7 years – <i>if not done in past 3 years</i>
U.S. National Criminal and Sex Offender Database – <i>if not done in past 3 years</i>
Global Security Search to include US Department of Commerce - Denied Persons List, Office of Foreign Assets Control (OFAC) - Specially Designated Nationals List, and other global databases of individuals and entities sanctioned for regulatory breaches, narcotics trafficking, terrorist activities, or other crimes – <i>if not done in past 3 years</i>
Employment Verification to include employer name, dates of employment, title, reason for separation and eligibility for re-employment for each employer for past 5 years – <i>if employed by HCL for less than 5 years and not previously done</i>

## 6.3 Enhanced Background Check

HCL will conduct a background check on all U.S. Personnel engaged after June 30, 2019 whose job functions require placement on the Federal Access Control List and who require a background check pursuant to Section III of the National Security Agreement, prior to such U.S. Personnel performing services for In-Scope Products delivered to U.S. Federal Government Customers. In addition, HCL will conduct a background check on existing U.S. Personnel on the Federal Access Control List who require a background check pursuant to CFIUS020 – CFIUS Access Control Policy and who have not previously gone through a standard background check pursuant to the corporate HCL Background Verification Policy. The background check will consist of the component checks listed in Table 2.

**Table 2: Component Checks for U.S. Personnel Engaged After June 30, 2019**

Social Security Number Verification
Address History
Criminal Search to include County, State and Federal Records for past 7 years
U.S. National Criminal and Sex Offender Database
Global Security Search to include US Department of Commerce - Denied Persons List, Office of Foreign Assets Control (OFAC) - Specially Designated Nationals List, and other global databases of individuals and entities sanctioned for regulatory breaches, narcotics trafficking, terrorist activities, or other crimes

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	91 of 93

Employment Verification to include employer name, dates of employment, title, reason for separation and eligibility for re-employment for each employer for past 5 years - *Current employer verification done after joining HCL*

## 6.4 Transferred IBM Employees

HCL will not conduct background checks for any Former IBM Employee acquired by HCL from IBM whose job functions require placement on the Federal Access Control List if such Former IBM Employee worked on the In-Scope Software Products during his/her tenure with IBM at the same level of access control. If such Former IBM Employee did not work on the In-Scope Software Products during his/her tenure with IBM at the same level of access control, HCL will conduct a background check for that Former IBM Employee pursuant to the requirements in Section 6.3.

HCL will validate the level of access control based on a review of the job function performed by each Former IBM Employee at the time they were acquired by HCL from IBM.

## 6.5 Review and Disposition of Background Verification Reports

The BGV team reviews and dispositions background check results. The BGV team refers any concerns/discrepancies to the BGV Council for adjudication.

Serious concerns/discrepancies relevant to job performance or workplace safety and security for a Prospective Employee may result in the rescinding of an offer or, if results are for existing Personnel, a referral to HR and legal counsel for further action, including a recommendation to the CFIUS Security Officer, who will make the final decision on Federal Access Control List eligibility.

If existing Personnel do not meet the background check standards set forth in this policy during the course of their employment with HCL, it may result in separation from HCL. Adverse findings will be disclosed to the concerned individual.

## 6.6 Unauthorized Use of Background Check Information

Unauthorized disclosure of information obtained through the background check process will be subject to appropriate disciplinary action up to and including termination of employment and prosecution.

# 7. Audit & Record Keeping


HCL complies with all federal, state and local guidelines regarding the storage and retention of background verification reports.

## 7.1 Background Check Reports

- All information obtained as part of background checks shall be held in strictest confidence.
- All information and documentation provided by any Prospective Employee and/or existing Personnel shall be retained by HCL for seven years.

Classification – Internal

Business Confidential Pursuant to 50 U.S.C. § 4565 - Protected from Disclosure Under 5 U.S.C. § 552

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	92 of 93


## 8. Related Documents

The following related documents are associated with this policy:

- 30. CFIUS020 – CFIUS Access Control Policy
- 31. [HCL Background Verification Policy](#)

## 9. Change Log

Version	Date	Author(s)	Summary of Changes
1.00	December 18, 2019	Paul Hudson Benson	Final document
1.00	January 15, 2020	Karen Plonty	Approved by the CFIUS Governance Committee without changes.

	CFIUS Security Policies	DOC.NO.	CFIUS100
	U.S. National Security Compliance	VER.NO.	1.00
		DATE	15-Jan-2020
		PAGE NO.	93 of 93

#### **EMPLOYEE ACKNOWLEDGEMENT**

I acknowledge that I have received and reviewed HCL's Committee on Foreign Investment in the U.S. (CFIUS) Security Policies.

I fully understand that I have an obligation to comply with HCL's CFIUS Security Policies, and that failure to follow the CFIUS Security Policies could result in possible disciplinary action up to and including termination of employment. I further acknowledge and affirm that:

1. In carrying out my responsibilities for HCL, I will comply fully with HCL's CFIUS Security Policies, including but not limited to policies that:
  - Restrict access to U.S. Federal Government Customer Data for HCL In-Scope Software Products to only U.S. Personnel, and
  - Require authorization on the Federal Access Control List for access to facilities, systems, databases, applications, information and job functions that are restricted to only U.S. Personnel.
  
2. In carrying out my responsibilities for HCL, I shall ensure that all records and documentation I am required to maintain are accurately and reliably recorded and reported.
  
3. I understand that HCL will not take retaliatory action against any HCL personnel who in good faith reports a suspected breach of the CFIUS Security Policies.
  
4. I will promptly report any question or concern about a suspected breach of CFIUS Security Policy to a CFIUS Implementation Leader or to [cfius@hcl.com](mailto:cfius@hcl.com), including but not limited to:
  - Any suspected unauthorized access to or disclosure of U.S. Federal Government Customer Data
  - Any suspected unauthorized access to the Secure Software Build Environment or Federal Support Environment
  - Any suspected compromise or unauthorized change to HCL In-Scope Software Product code
  - Any violation of the CFIUS Security Policies or Cybersecurity Plan for the Secure Software Build Environment and Federal Support Environment

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Employee Name (printed)