

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 78 PAGES

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

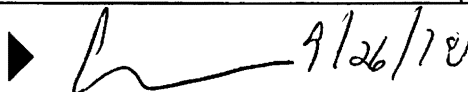
1. DATE OF ORDER		2. CONTRACT NO. (If any) HSHQDC-14-D-E2042		6. SHIP TO:	
3. ORDER NO. 70SBUR18F00000703		4. REQUISITION/REFERENCE NO. TFM180017		a. NAME OF CONSIGNEE Department of Homeland Security	
5. ISSUING OFFICE (Address correspondence to) USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403				b. STREET ADDRESS US Citizenship & Immigration Svcs Office of Information Technology 111 Massachusetts Ave, NW Suite 5000	
				c. CITY Washington	e. ZIP CODE 20529
7. TO:				f. SHIP VIA	
a. NAME OF CONTRACTOR LEIDOS INNOVATIONS CORPORATION				8. TYPE OF ORDER	
b. COMPANY NAME				<input type="checkbox"/> a. PURCHASE	
c. STREET ADDRESS 9221 CORPORATE BLVD				REFERENCE YOUR: Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.	
d. CITY ROCKVILLE				e. STATE MD	f. ZIP CODE 20850
9. ACCOUNTING AND APPROPRIATION DATA See Schedule				10. REQUISITIONING OFFICE USCIS Contracting Office	
11. BUSINESS CLASSIFICATION (Check appropriate box(es)) <input type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM <input type="checkbox"/> h. EDWOSB				12. F.O.B. POINT Destination	
13. PLACE OF		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	
a. INSPECTION Destination	b. ACCEPTANCE Destination			16. DISCOUNT TERMS Net 30	

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 080285808 Clauses incorporated by reference: 52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) Continued ...					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(h) TOTAL (Cont. pages)
	21. MAIL INVOICE TO:						
	a. NAME See Invoicing Instructions						17(i) GRAND TOTAL
	b. STREET ADDRESS (or P.O. Box)						
c. CITY			d. STATE	e. ZIP CODE			

22. UNITED STATES OF
AMERICA BY (Signature)

 9/26/18

23. NAME (Typed)
Chad R. Parker
TITLE: CONTRACTING/ORDERING OFFICER

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE NO

2

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	<p>This is a Hybrid Task Order for Outcome-Based Delivery and DevOps Services (ODOS II)</p> <p>This order is subject to the terms and conditions to the EAGLE II contract # HSHQDC-14-D-E2042.</p> <p>AAP Number: none DO/DPAS Rating: NONE</p> <p>Period of Performance: 09/30/2018 to 09/29/2021</p>					

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

3

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

4

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

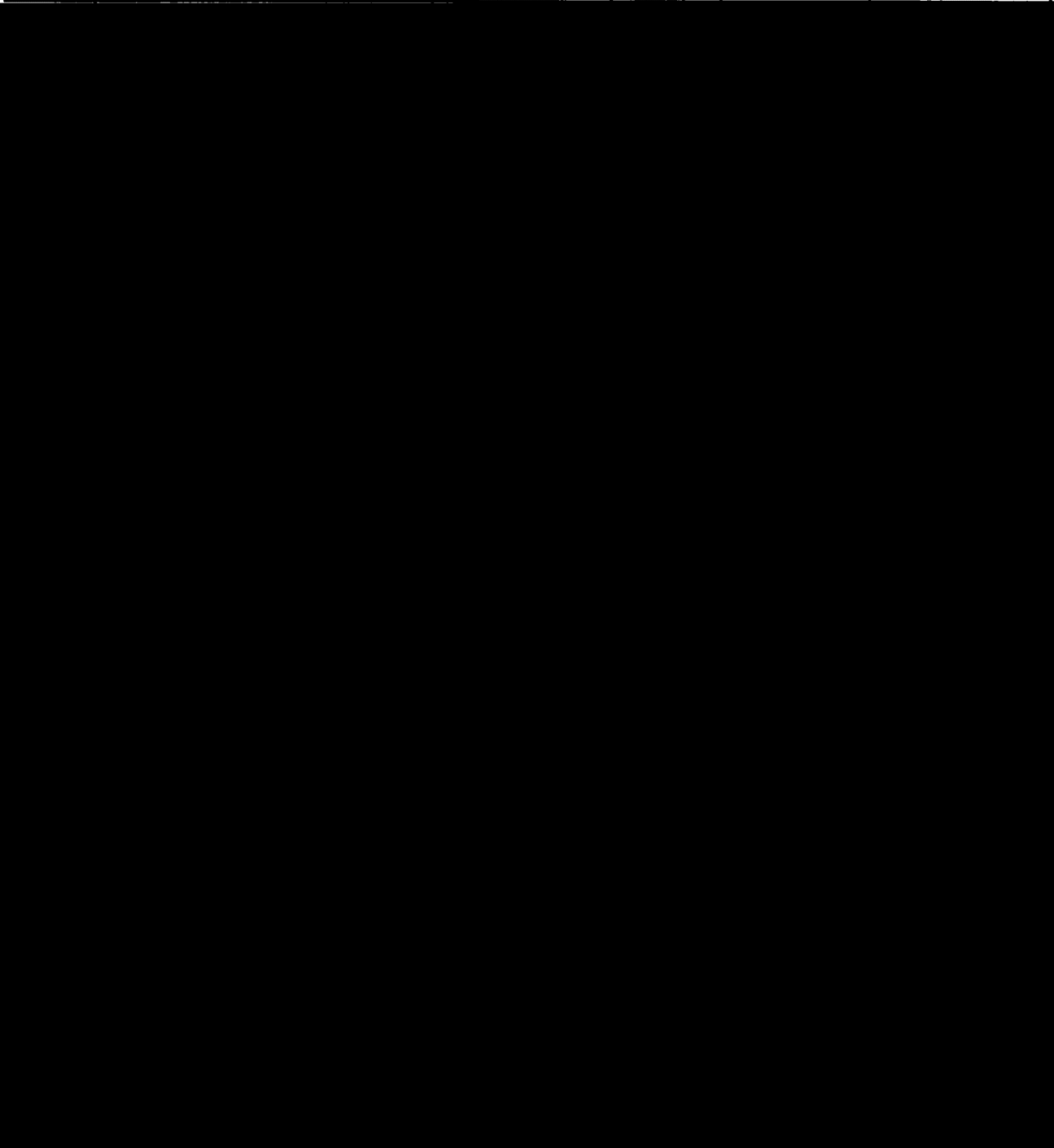
CONTRACT NO.

HSQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------



TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

FORM 348 (Rev 4/2006)

Prescribed by GSA FAR (48 CFR) 53.213(f)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

5

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

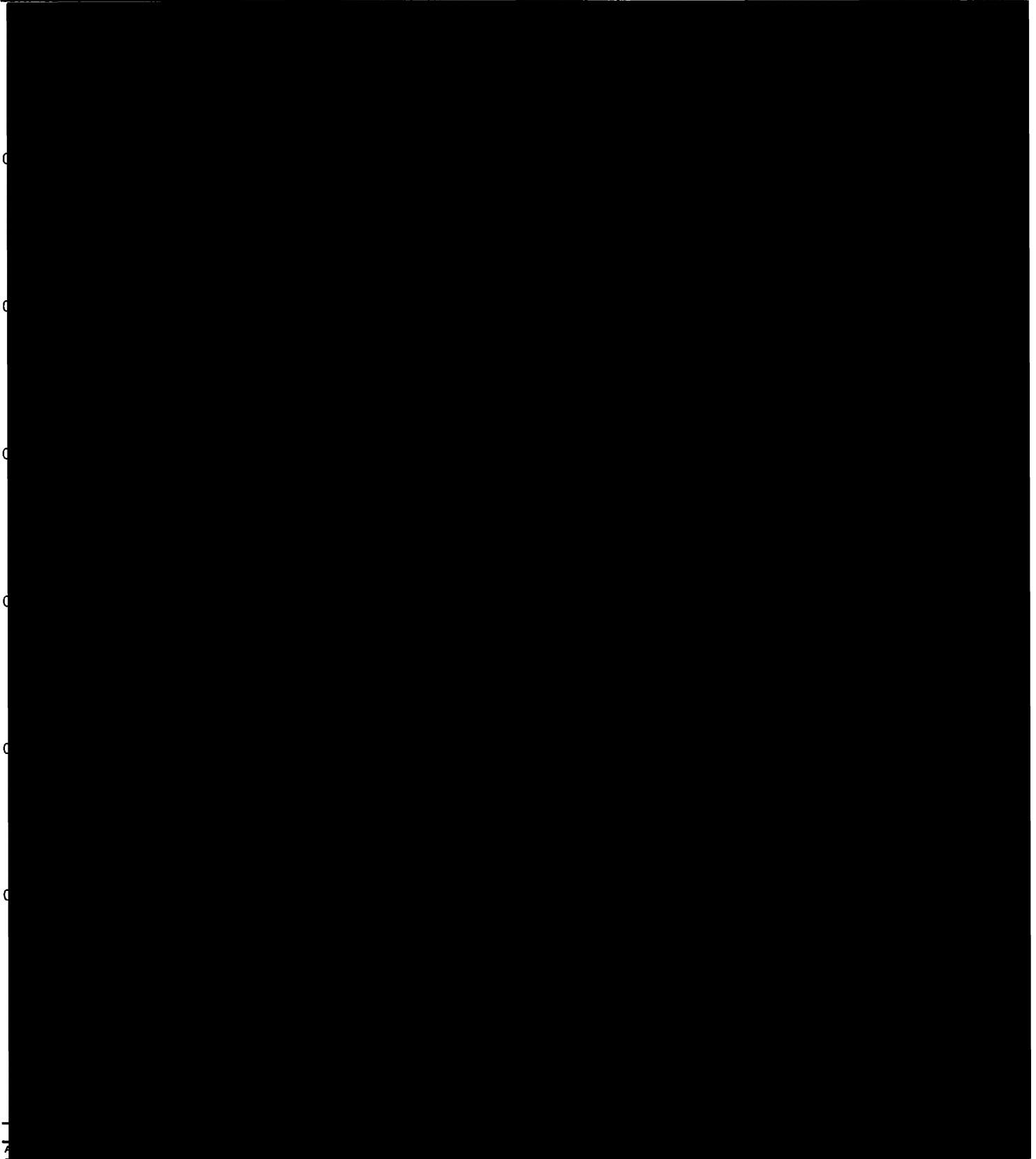
CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------



ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

6

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

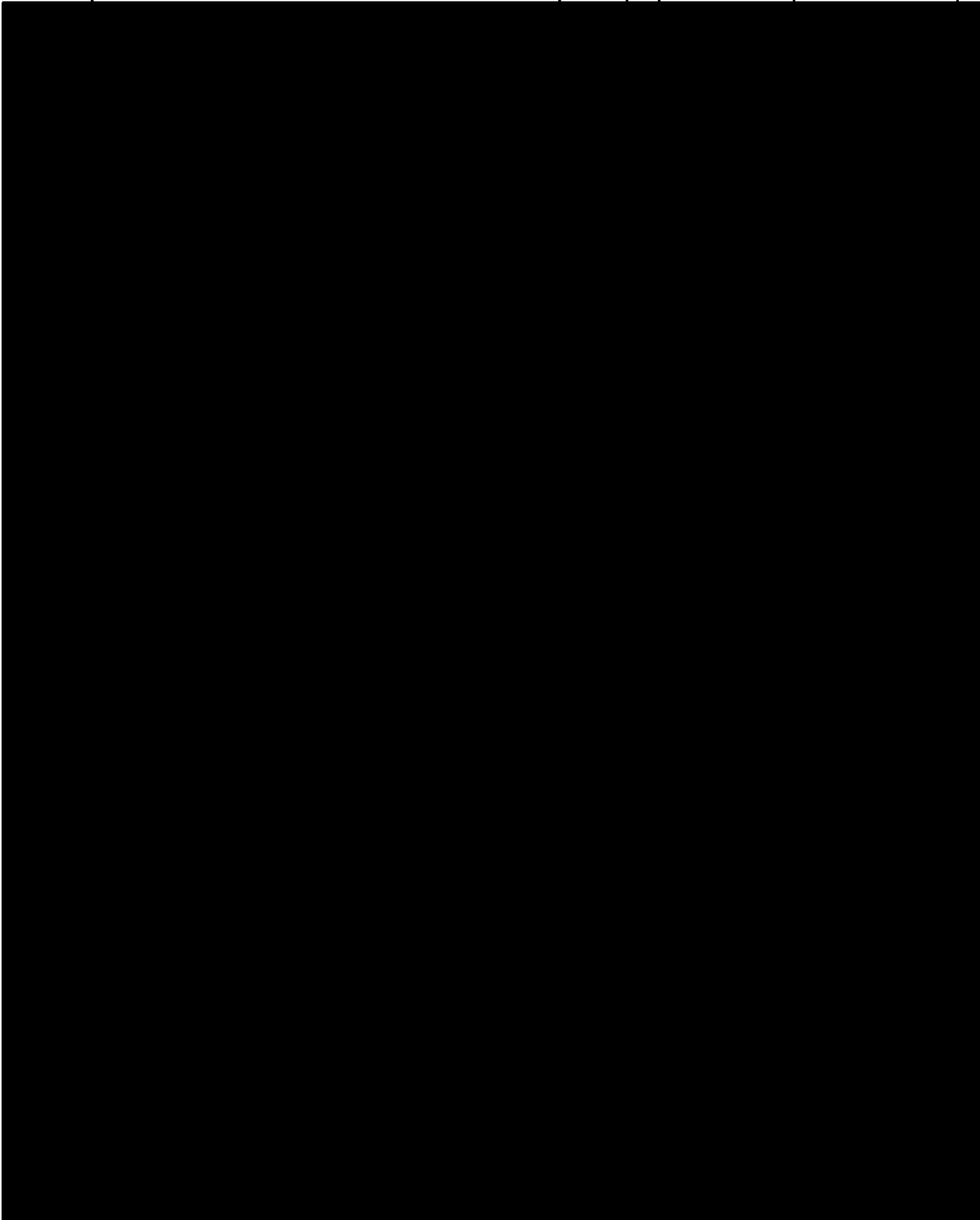
CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED
(a)	(b)	(c)	(d)	(e)	(f)	(g)



FORM 348 (Rev. 4/2006)

Prescribed by GSA FAR (48 CFR) 53.213(f)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

7

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

8

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY

UNIT

UNIT

AMOUNT

QUANTITY

(a)

(b)

ORDERED

(d)

PRICE

(e)

(f)

ACCEPTED

(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

9

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

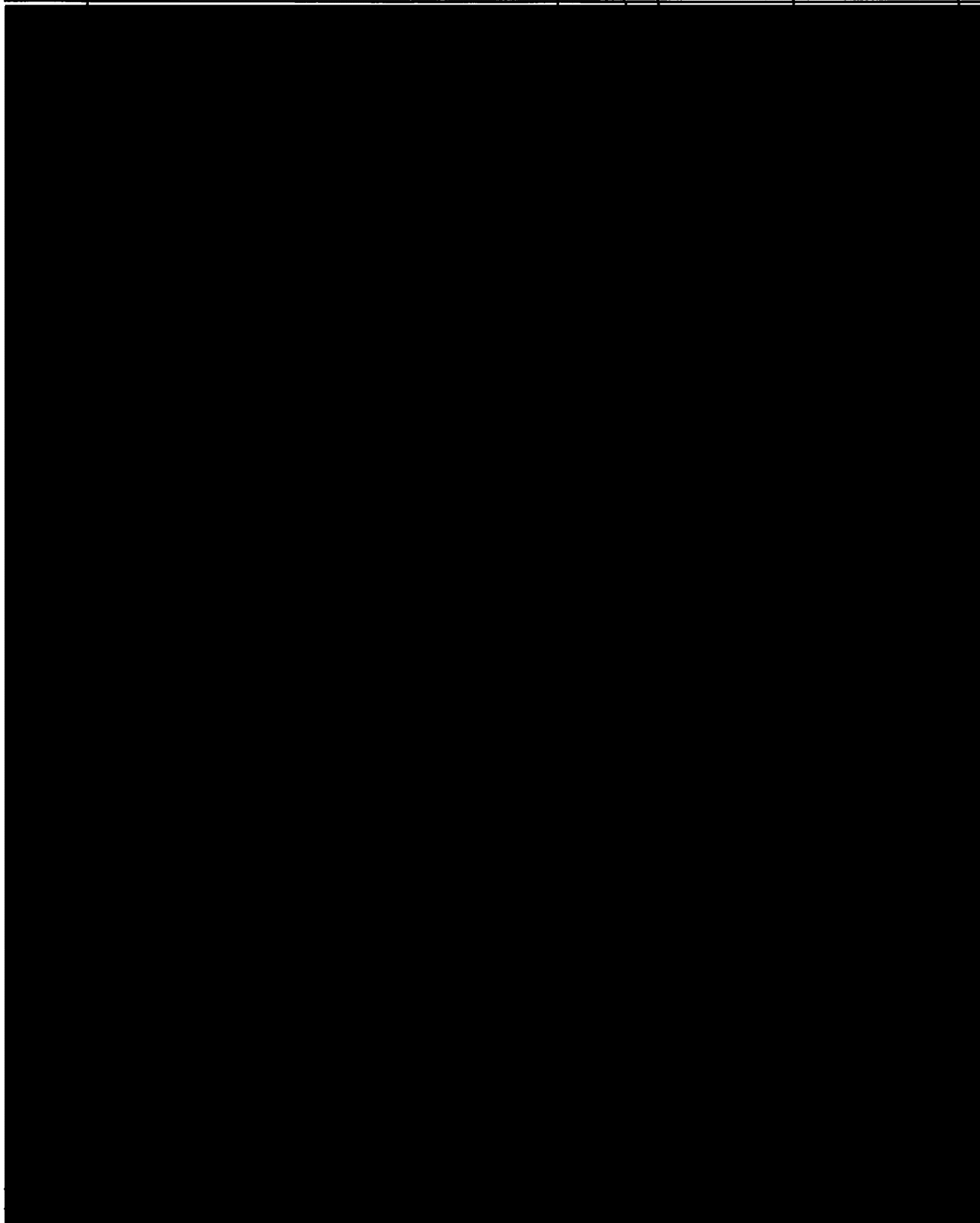
CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------



ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
10

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

11

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------

PAGE NO
12

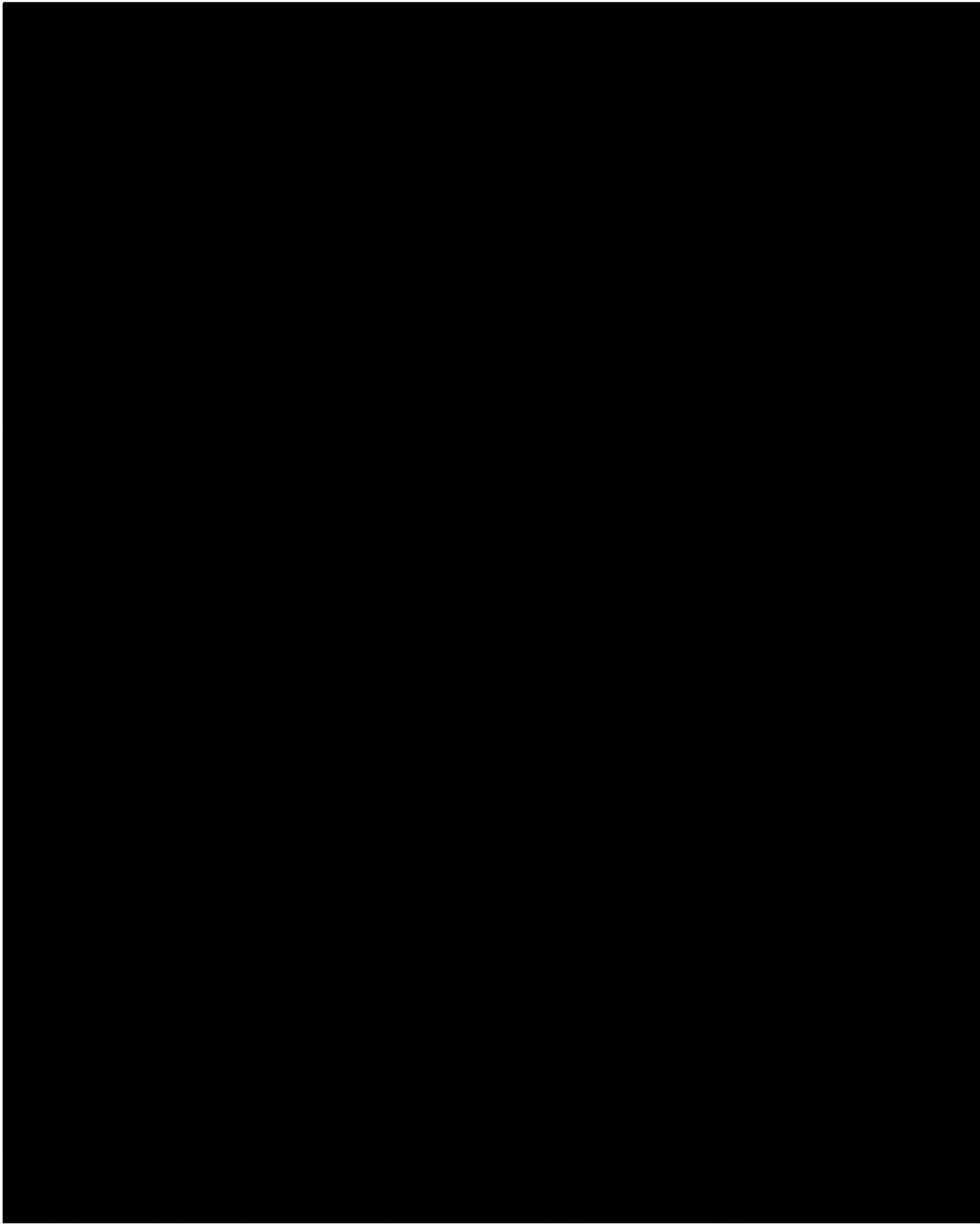
DATE OF ORDER

CONTRACT NO.

ORDER NO.

70SBUR18F00000703

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED
(a)	(b)	(c)	(d)	(e)	(f)	(g)



ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

14

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

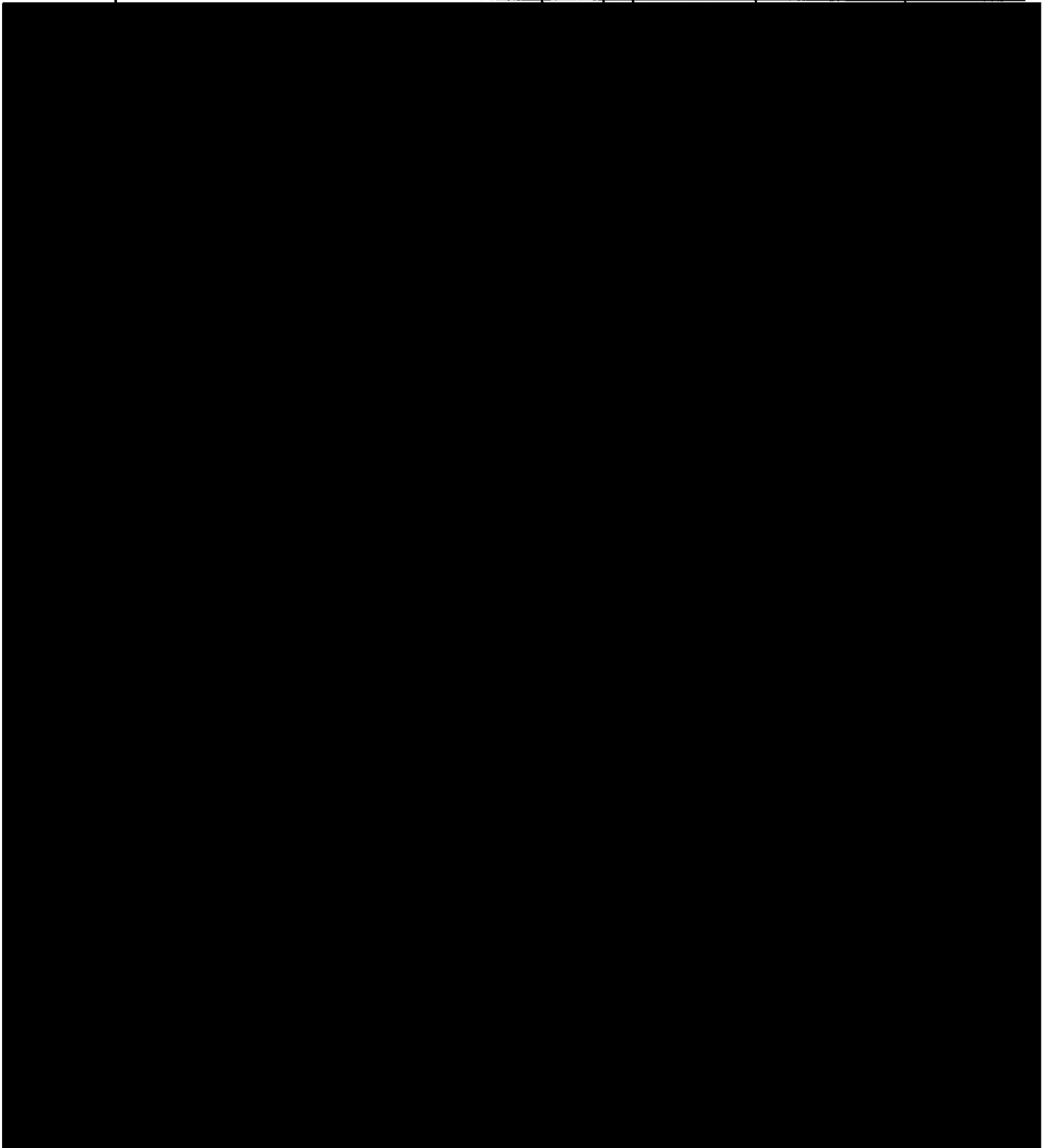
CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED
(a)	(b)	(c)	(d)	(e)	(f)	(g)



ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

15

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY

UNIT

UNIT

PRICE

AMOUNT

QUANTITY

ACCEPTED

(a)

(b)

ORDERED

(c)

(d)

(e)

(f)

(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

16

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

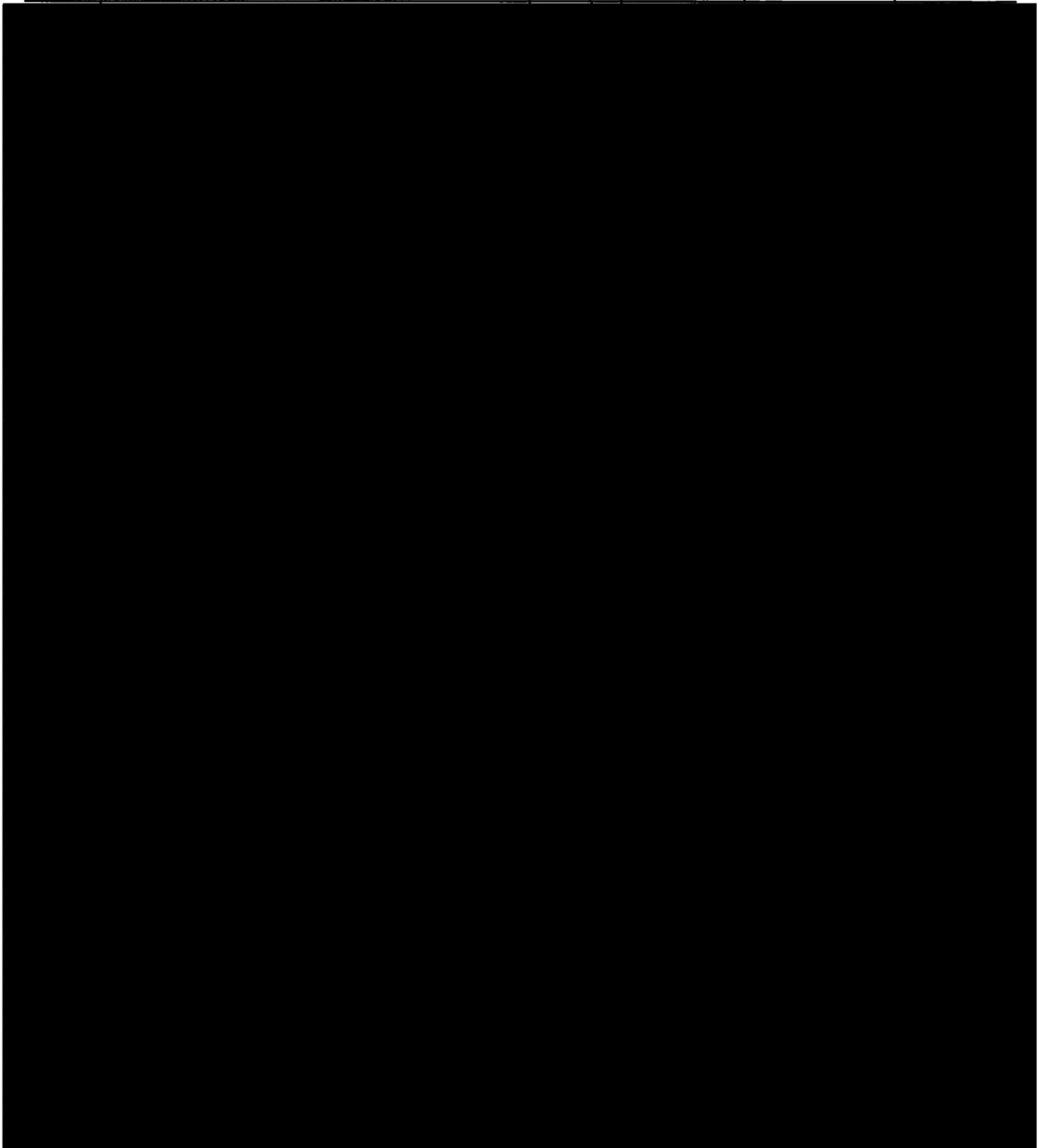
CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED
(a)	(b)	(c)	(d)	(e)	(f)	(g)



ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
18

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED
(a)	(b)	(c)	(d)	(e)	(f)	(g)

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

\$0.00

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 348 (Rev. 4/2006)
Prescribed by GSA FAR (48 CFR) 53.213(f)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

15

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

16

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

\$0.00

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 348 (Rev 4/2006)
Prescribed by GSA FAR (48 CFR) 53.213(f)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

17

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY

UNIT

UNIT

PRICE

AMOUNT

QUANTITY

ACCEPTED

(a)

(b)

ORDERED

(c)

(d)

(e)

(f)

(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

18

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED
(a)	(b)	(c)	(d)	(e)	(f)	(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

19

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY
ORDERED

UNIT
(d)

UNIT
PRICE

AMOUNT

QUANTITY
ACCEPTED

(a)

(b)

(c)

(d)

(e)

(f)

(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
20

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY
ORDERED

UNIT

UNIT
PRICE

AMOUNT

QUANTITY
ACCEPTED

(a)

(b)

(c)

(d)

(e)

(f)

(g)

ORDER FOR SUPPLIES OR SERVICES

PAGE NO

SCHEDULE - CONTINUATION

21

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY

UNIT

UNIT

AMOUNT

QUANTITY

(a)

(b)

ORDERED
(c)

(d)

PRICE
(e)

(f)

ACCEPTED
(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
22

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY

UNIT

UNIT

PRICE

AMOUNT

QUANTITY

ACCEPTED

(a)

(b)

(c)

(d)

(e)

(f)

(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

23

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY
ORDERED

UNIT

UNIT
PRICE

AMOUNT

QUANTITY
ACCEPTED

(a)

(b)

(c)

(d)

(e)

(f)

(g)

PAGE NO
24

DATE OF ORDER

CONTRACT NO.

ORDER NO.

70SBUR18F00000703

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED
(a)	(b)	(c)	(d)	(e)	(f)	(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

25

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY

UNIT

UNIT

PRICE

AMOUNT

QUANTITY

ACCEPTED

(a)

(b)

ORDERED

(c)

(d)

(e)

(f)

(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

26

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY

UNIT

UNIT

AMOUNT

QUANTITY

(a)

(b)

ORDERED

(d)

PRICE

(e)

(f)

ACCEPTED

(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

27

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

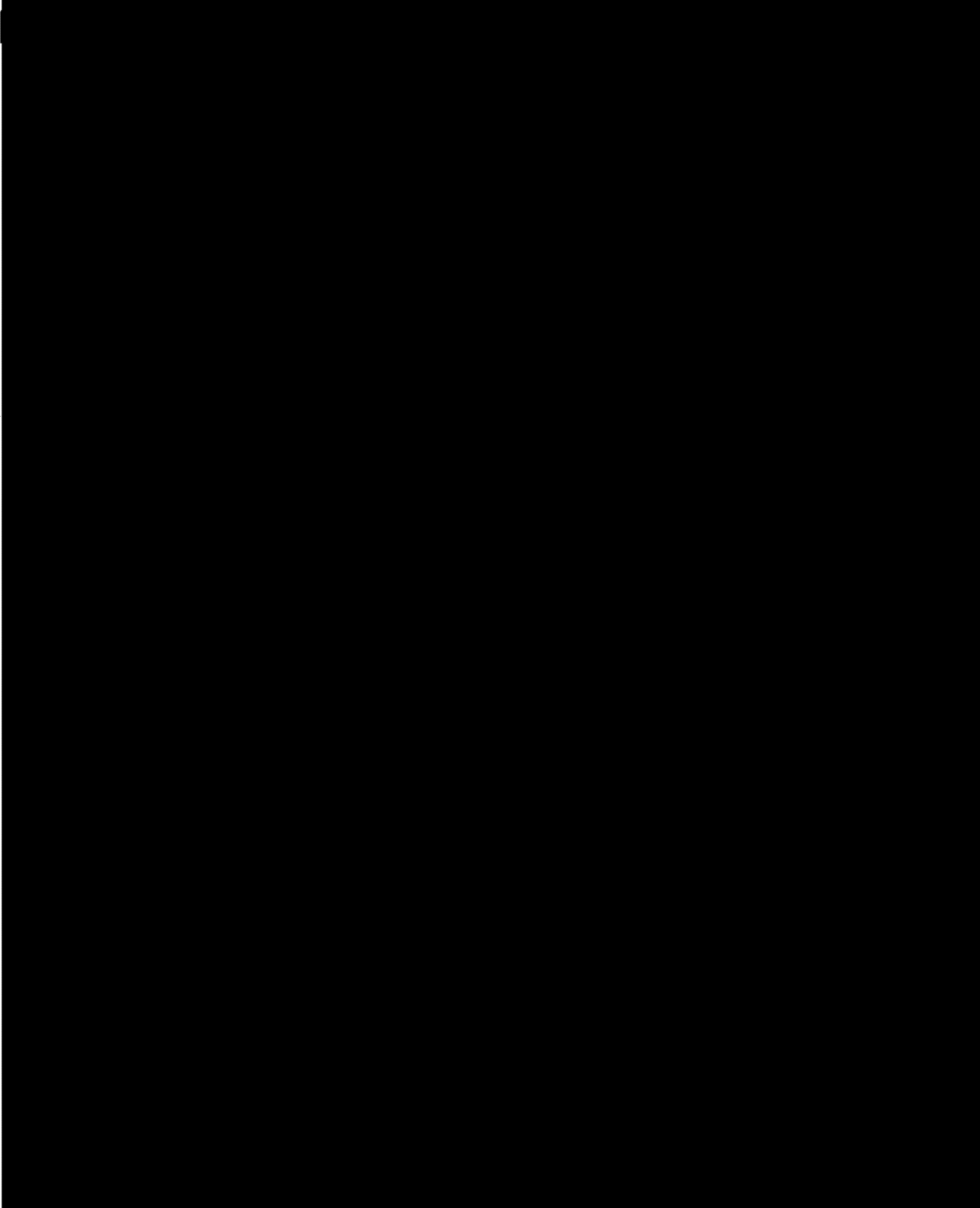
CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------



PAGE NO
28

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED
(a)	(b)	(c)	(d)	(e)	(f)	(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

29

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY

UNIT

UNIT

PRICE

AMOUNT

QUANTITY

ACCEPTED

(a)

(b)

ORDERED

(c)

(d)

(e)

(f)

(g)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
30

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO.

SUPPLIES/SERVICES

QUANTITY
ORDERED
(c)

UNIT
(d)

UNIT
PRICE
(e)

AMOUNT

(f)

QUANTITY
ACCEPTED
(g)

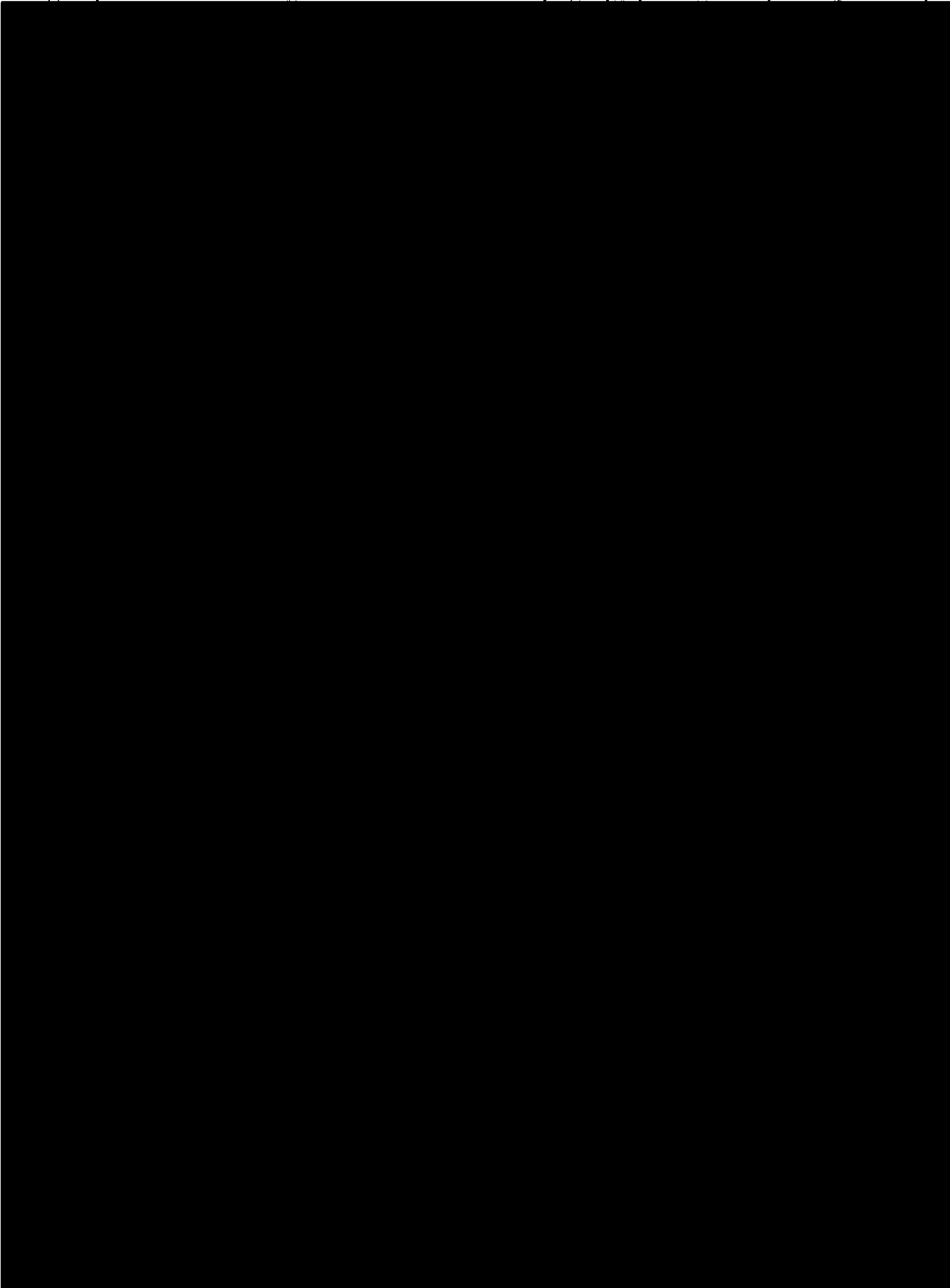
(a)

(b)

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO. HSHQDC-14-D-E2042	ORDER NO. 70SBUR18F00000703
---------------	-----------------------------------	--------------------------------

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED (g)
----------	-------------------	---------------------	------	---------------	--------	-----------------------------



PAGE NO
32

DATE OF ORDER

CONTRACT NO.

ORDER NO.

70SBUR18F00000703

ITEM NO.	SUPPLIES/SERVICES	QUANTITY ORDERED	UNIT	UNIT PRICE	AMOUNT	QUANTITY ACCEPTED
(a)	(b)	(c)	(d)	(e)	(f)	(g)

ORDER FOR SUPPLIES OR SERVICES

PAGE NO

SCHEDULE - CONTINUATION

33

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

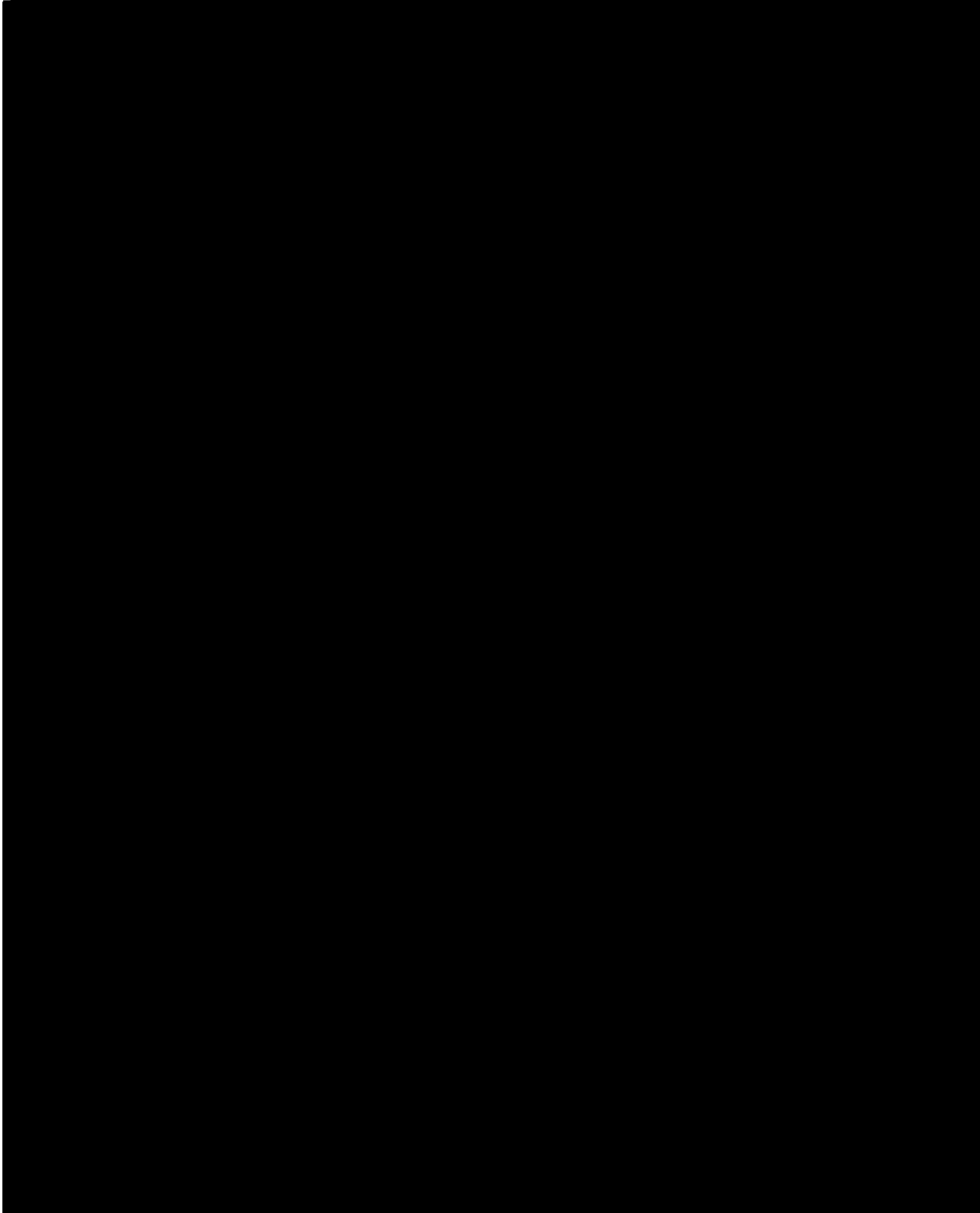
CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------



ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO

34

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

HSHQDC-14-D-E2042

ORDER NO.

70SBUR18F00000703

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
-----------------	--------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------

SECTION C – DESCRIPTION/SPECS/WORK STATEMENT

Outcome-Based Delivery and DevOps Services (ODOS) II (Performance Work Statement)

1. OVERVIEW

U.S. Citizenship and Immigration Services (USCIS) Office of Information Technology (OIT) is seeking to acquire highly qualified Development and Operations (DevOps) teams. Outcome-Based Delivery and DevOps Services (ODOS) II will be part of an ecosystem, participating with federal employees, and other contractors, in a team-based DevOps approach to deliver mission value frequently, cost-effectively, responsively, and with high quality.

The Government will oversee the architecture and design of the system. The ODOS II contractors will be responsible for developing high quality business functionality to work within those architectures to meet the business capabilities.

2. AGENCY MISSION AND GOALS

U.S. Citizenship and Immigration Services administers the nation's lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.

3. SCOPE

The scope of this task order is for the Contractor to deliver (ELIS and Non-ELIS) related DevOps services. The high-level requirements detailed in Section 5 must be met in order to fulfill the objectives of this task order, and may be refined adaptively over the course of the effort to continuously meet specified user needs.

4. TECHNICAL LANDSCAPE

The USCIS technical landscape has shifted from a costly, proprietary, COTS-based framework to a wide adoption framework that is based on the open source platform. With this shift, the current USCIS architecture has demonstrated success with a stack of predominately open source tools that are currently under consideration for standardization across development teams at USCIS.

Development teams are empowered to manage the Continuous Integration/Continuous Delivery (CI/CD) process completely, and have the ability to deploy multiple times a day with zero downtime to the system.

Open Source solutions and platform agnostic software is employed wherever possible to create the possibility of more easily deploying solutions in Amazon Web Services (AWS). Besides maintaining the integrated CI/CD environment in the AWS environment, OIT continues to focus on new initiatives to enhance the development with containerized Microservices on OpenShift Container Platform, configuring Hygieia monitoring tool, API Gateway configuration, etc.

Team members are expected to gain understanding of the technical landscape so they can effectively advocate for technology solutions that benefit users.

Current Development and Test Tool Suite			
Name	Version	Manufacturer	Function
ActiveMQ	15.4.5	Apache	Messaging
Adobe Livecycle	11.0.0	Adobe	PDF document generation
Amazon Web Services	Latest	Amazon	Cloud computing services
AngularJS	1.2	AngularJS	Javascript Framework
Ansible	v2.3.1.0-1	OSS GNU	Open Source simple IT automation platform
Apigee	14.17.05	Google	CLOUD NATIVE API Management Platform for ensuring security, visibility, and performance across the entire API landscape (pending for procurement).
Chef	11.4	Opscode	Open source software deployment
Cloudbees Jenkins	2.46.30	Cloudbees	Commercial continuous integration server to build declarative pipelines.
Confluence	5.10.2	Atlassian	Documentation Wiki
Docker	1.12.6	Docker Inc	Software containerization and deployment
Eclipse	Neon	Eclipse	IDE for software development
Fortify	17.10	HP	Static Code Analysis
GitHub Enterprise	2.12.8	GitHub	Hosted code management
GitRob	1.1.12	MIT	Open Source Reconnaissance tool for GitHub
Gradle	2.13	Gradle.org	Open source build automation tool
Hibernate	4	Jboss	Open source object / relational mapping library for Java
Hygieia	2.0.5	CapitalOne	(Also called “devops-dashboard”) Configurable dashboard to visualize near real-time status of delivery pipeline, JIRA integration for status on your user stories, and defects tracking.
Java	1.8	Oracle	Language for software development
Jboss Application Server	7.0.2	Jboss	Open source application server
Jboss Rules Engine	5	Jboss	Open source rules engine
Jenkins	2.89.4	Jenkins CI	Open source continuous integration server

Current Development and Test Tool Suite			
Name	Version	Manufacturer	Function
Jira	7.3.6	Atlassian	COTS ALM tool
Junit	LATEST	Apache	Unit testing
KeePass	2.36	KeePass	Password Management tool
Kong	0.10.3	Mashape	API Gateway Layer Software
Liquibase	3.0.5	Liquibase.org	Open source database source code control
MongoDB	3.4.2	10gen, Inc	Open source document oriented database system
Nexus	3.3.0-01	Sonatype	Open source repository manager
Obsidian	4.3.0	Carfey	Scheduler
OpenShift Enterprise	3.6.1.17	RedHat	Container Platform/Orchestration tool
Oracle Database	11.2.0.4.v15	Oracle	Commercial database
OWASP	LATEST	Creative Commons	Open Web application Security Project
PostgreSQL	9.6.6	OpenSource	Permanent data source
Selenium	LATEST		Browser testing in Firefox
Slack	LATEST SAAS	Slack	Collaboration tool
SonarQube	6.2	Maintained by SonarSource	OSS Static Code Analysis
Spring Framework	4.2	SpringSource.org	Open source Java framework
Terraform	0.9.8	HashiCorp	Infrastructure as Code aid
Twistlock	2.0	Twistlock	Container Vulnerability Scanning
WebInspect	17.1	Hewlett Packard	Dynamic security testing application

Table 1: Current Development and Test Tool Suite

5 TASKS

The contractor's responsibilities will be to empower DevOps teams to deliver innovative and secure solutions that adapt to the changing business needs, and to be efficient at delivering business results. The tasks identified in the following sections describe the work that will occur in order to accomplish the vision. ODOS II contractors shall provide teams that are able to perform the tasks as described, while conforming to the expectations, expertise, and abilities in the technologies stated but not limited to those listed in section 4 TECHNICAL LANDSCAPE

As the technical landscape evolves, the skills of the contractor's teams must also evolve.

The contractor shall provide qualified DevOps teams who have relevant experience and domain knowledge in line with the performance work statement.

The contractor shall provide DevOps teams capable of utilizing best DevOps practices in IT development, security integration, and maintenance efforts for sustaining the system. The ODOS II contractors will be working in a DevOps framework and shall be proactive in monitoring and maintaining the system in production.

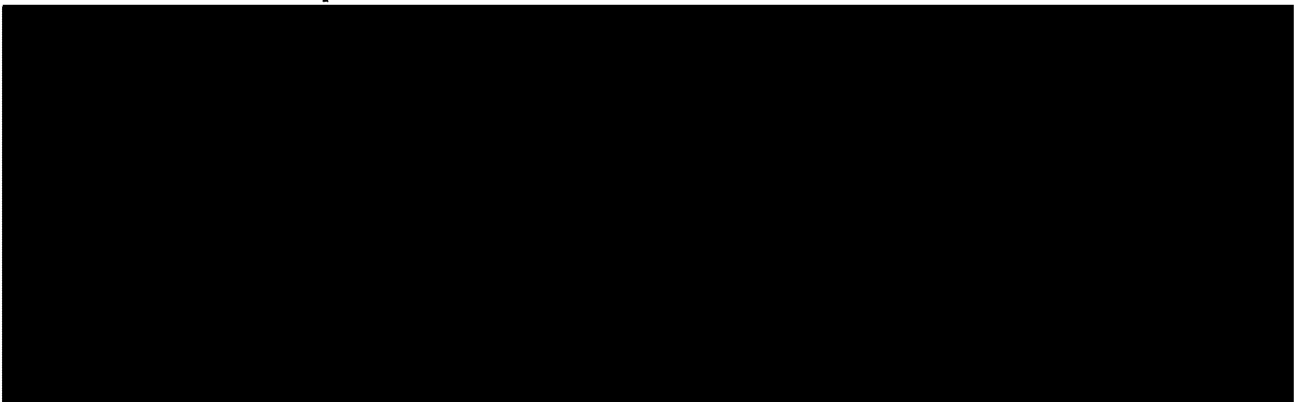
The contractor shall be responsible in the delivery of code from creation, to running in the pipeline, to deployment, and sustainment.

As DHS requires Section 508-compliant user interfaces, the contractor shall employ an accredited member of each DevOps team as a DHS trusted Section 508 tester. The Section 508 Accessibility requirements are listed in Section H.28 Information Technology Accessibility for Person with Disabilities of the EAGLE II contract. Please refer to <https://www.dhs.gov/trusted-tester> for more information.

The Contractor must provide a quarterly report that lists the contract name, number, and COR with each Trusted Tester's name, certification level, certification date, certification number, E-mail address, phone number, and supported projects to the COR and USCIS Section 508 Coordinator. This report must also be provided within 10 working days of any change in the Trusted Tester population.

The contractor's work shall conform to the architecture and design provided by the USCIS Architecture and Design team and the DevOps processes set up by the USCIS Processes and Practices team that will be provided after award.

5.1 Provide DevOps Teams



5.2 Development

- a) The contractor shall provide rapid delivery in small batches, increasing the frequency and pace of releases, applying the continuous integration and continuous delivery practices.
- b) The contractor shall integrate security into the DevOps workflow in a collaborative way by employing a "DevSecOps" approach, and deliver the system with built-in security.
- c) Each member of the contractor's team shall be responsible for security.

- d) The contractor shall employ design patterns that enable code simplicity, user's needs, and future maintainability.
- e) The contractor shall employ microservice architecture on OpenShift Platform, as a design approach, to build applications as a set of small services, organized into aggregates, with transactional consistency.
- f) The contractor shall employ Infrastructure as Code (IAC) as a practice enabling the cloud's Application Programming Interface (API)-driven model to interact with infrastructure programmatically.
- g) The contractor shall have estimation and planning skills for analyzing user stories for size and requirements.
- h) The contractor shall be responsible for providing continuous production support and maintenance.
- i) The contractor shall develop monitoring, alerting systems, and logging practices to help stakeholders stay informed of performance in real-time.
- j) The contractor shall incorporate monitoring solutions like Hygieia, New Relic, etc. The contractor may suggest new methods or tools; however, developers shall add health checks to code so that monitoring tools can detect changes with appropriate metrics.
- k) The contractor shall ensure that the system complies with the Agency's security policies in order to safeguard the system against external and insider threats.
- l) The contractor shall ensure that teams implement proactive approaches to reduce vulnerabilities and to improve responsiveness to unforeseen events.
- m) The contractor shall ensure that the system has quality build-in, by prioritizing Availability, Maintainability, Vulnerability, and Reliability.
- n) The contractor shall collaborate and cooperate with government and other contractor teams to improve the user experience, to baseline and re-establish key performance parameters for the system, and to address all gaps as part of continuous improvement and collaboration.
- o) The contractor shall immediately fix any escaped defects that have a significant impact on business operations.
- p) The contractor shall adopt USCIS design and coding standards in the course of their application development.
- q) The contractor shall provide technical methods, techniques, and concepts that are innovative, practical, cost-effective, and conducive to the Agency's processes and quality standards.
- r) The contractor shall develop applications based on requirements that are evolving and emerge as the business climate shifts.

5.3 Code Quality, Security and Standards Compliance

- a) The contractor shall develop high quality secure code and is responsible for any technical debt (design debt or code debt), that is incurred as a result of their development activities.
- b) The contractor shall proactively assist the government in eliminating existing technical debt and rewriting issues to remove bad designs and security issues from the code base.
- c) The contractor's work shall conform to the architecture and security standards established by the USCIS Enterprise Architecture team.
- d) The contractor's system design shall be adaptive to volatile system requirements.
- e) The contractor shall design, develop, and deploy software in accordance with industry best practices. This includes, but is not limited to, following 12 Factor App development practices (12factor.net), cloud native (cncf.io), NIST Risk Management Framework, building/deploying microservices on OpenShift Platform, and deploying software with zero downtime. The contractor shall stay fluent with industry best practices as they evolve.
- f) The contractor's code shall meet the functional and Non-functional Requirements (NFR), such as performance, security, and capabilities meet database development requirements, meet testing requirements, and are deployable and fully tested in preparation for USCIS OIT IV&V review.

5.4 Test, Integration and Deployment

- a) The contractor shall be responsible for creating test cases, automated test scripts to support test automation activities, and thoroughly testing the code.
- b) The contractor shall collaborate with other teams to support test-driven and continuous code integration.
- c) The contractor shall share test scripts (manual and automated) as needed with other testing entities.
- d) The contractor shall work to increase the code coverage, the degree to which the source code of a program is executed when a particular test suite runs, and quality, as specified by government leadership.
- e) The contractor shall perform alpha and beta testing.
- f) The contractor shall assist with constructing validation steps (both positive and negative testing) for user acceptance testing on an as needed basis.
- g) The contractor shall support the activities of the Integration and Configuration team to ensure the automatic build and deployment process works effectively across all environments, including the contractor's development/test enclave. Deployment and testing in the development/test environment should mimic closely the actions performed for deployment and testing in staging and production. The contractor will leverage the OpenShift Platform to the fullest extent possible.

- h) The contractor shall thoroughly test changes and remediate all known security issues before committing them into the CI pipeline.
- i) The contractor shall use their DevOps personnel to perform deployments of some or all code directly to production, as directed by the Government.
- j) The contractor shall not depend on independent inspections to achieve quality and security.

5.5 Quality Control

- a) The contractor shall create a Quality Management Plan.
- b) The contractor shall ensure development related activities are in accordance with the contractor's Quality Management Plan.

5.6 Operations

- a) The contractor shall respond to production incidents, including but not limited to breakages of functionality, system outages, performance problems, security incidents, or user complaints. This responsibility includes, but is not limited to, investigating and triaging incidents, rolling systems back to earlier states, developing and deploying fixes (on software they may or may not have developed), engaging with other contractors and federal employees to fix related systems, and running incident retrospectives to ensure permanent fixes.
- b) The contractor shall be responsible for the operation in production of the capabilities they develop.
- c) The contractor shall build monitoring triggers to effectively reveal production issues in a timely fashion.
- d) The contractor shall provide root cause analysis on all outages with actionable recommendations on how to prevent issues going forward.
- e) The contractor shall have technical skills and expertise as necessary to provide production support.
- f) The contractor shall ensure streamlined operations to make processes more efficient.
- g) The contractor shall build application health monitoring and alerting functions into the system, to ensure system is monitored effectively, to reveal any production issues, when they happen.
- h) The contractor shall ensure that the system is monitored to reveal user analytics and interactions, and provide the capability to automatically report on such activities.
- i) The contractor shall ensure that there is an automated way to monitor for dependency and network-related production issues, providing the capability to rule out application issues.
- j) The contractor shall continuously refine and improve every process, while simultaneously reducing the likelihood of major outages.

5.7 Administrative Activities

- a) The contractor shall collaborate with stakeholders, support contractors, and third party vendors throughout system integration, performance, security, Section 508, system acceptance, user acceptance, usability, and test and evaluation reporting.
- b) The contractor shall manage all contractor resources, and supervise all contractor staff in the performance of work on this task order. The contractor shall manage and coordinate its team(s) on a day-to-day basis, and ensure plans are communicated to team members. Likewise, the contractor must ensure that the health and progress against those plans are adequately reported.
- c) The contractor shall organize, direct, and coordinate planning and execution of all task order activities.
- d) Vehicles for transparency, such as the USCIS Application Lifecycle Management (ALM) tool, shall be maintained with data so that reports and charts can be generated as needed, and so that user stories, defects, and tasks and their status are available to stakeholders. Task boards and SharePoint sites, meetings, and demos shall be used to share information and report progress.
- e) The contractor shall have lean documentation as part of the definition of done.

6 KEY PERSONNEL

Key Personnel are required for successful performance of this task order. The contractor shall provide statements of qualifications for individuals identified as key personnel within ten (10) calendar days after the date of the award. These qualifications will be based on the EAGLE II labor categories listed under section I.4 HSAR Clause 3052.215-70 Key Personnel or Facilities. The Management Lead shall be a current full time employee of the prime contractor. The contractor may fill the Technical Lead position with a subcontractor. The contractor shall identify key personnel who shall be the Management Lead for the task order as a whole and one Technical Lead for every four teams.

The Management Lead shall ensure that all work on this contract complies with contract terms and conditions, and shall have access to contractor corporate senior leadership when necessary. The contractor's Management Lead shall be the primary interface with the USCIS Contracting Officer's Representative (COR) and Contracting Officer (CO), shall attend status meetings and ad hoc meetings with stakeholders, and shall be accompanied by the Technical Lead(s) when requested. The Management Lead shall be a single point of contact for resolution of contract related issues.

The Technical Leads must have extensive expertise in the DevOps development methodology and experience using many of the tools included in the Development/Test Tool Suite identified previously. They will also be the lead on the requirements, design, development, testing, implementation, and documentation of enhancements. Technical leads will also evaluate technical trends and provide recommendations for technology and architecture to meet business objectives.

7 TRANSITION

7.1 Transition Task

Transition shall occur in three phases.

In the first phase of transition (1 month PoP), the Government will issue a Notice to Proceed (NTP) for the management lead and one technical lead for a total of two (2) FTEs to participate in transition activities.

In the second phase (1 month PoP), a NTP will be issued to the five (5) Firm Fixed Price FTEs per team (10 personnel) once they have received an EOD approval.

In the third phase (1 month POP), a NTP will be issued to four (4) T&M FTEs per team (8 personnel) once they have received an EOD approval.

At the completion of transition (3 months POP), the contractor shall receive a NTP for Full Performance, which requires 100% staffing for each DevOps Team.

If needed the additional technical leads shall be included in the NTP for teams #5, 9 and 13.

The contractor shall provide a Transition Plan once approved by the government. The plan will document the technical requirements, responsibilities, transition management and resources, milestones, progress reporting, metrics, interfaces, subcontracts and license agreements (if any), equipment, tools, documentation, testing, training, and any support utilities and dashboards according to the Government template. The plan will describe any external dependencies and needs, including government furnished material or services.

7.2 Transition Support

The incoming contractor shall fully support work that is turned over by the outgoing contractor. The incoming contractor shall coordinate with the incumbent contractor during transition planning, and shall comply with transition milestones and schedules of events.

The incoming contractor shall be responsible for coordinating with the outgoing contractor during implementation of the transition and application cutover activities. The transition shall cause no disruption in development services or operations. To ensure the necessary continuity of services, and to maintain the current level of support, USCIS may retain services of the outgoing contractor for some, or all of, the transition period, as may be required.

As part of the transition, the incoming and outgoing contractors shall be expected to collaborate on the following:

- Inventory and orderly transfer of all Government-Furnished Property (GFP), to include hardware, software, and licenses, Contractor Acquired Government Property, and Government Furnished Information (GFI);
- A status of all deliverables;
- The transfer of documentation currently in process;
- The transfer of all software code in process;
- Certification that all non-public DHS information has been purged from any contractor-owned system;
- The exchange of accounts to access software and hosted infrastructure components;
- Participating in knowledge transfer activities in accordance with the transition plan;
- Providing members to, and participate in, transition management team;

- Updating the library of production support and performance dashboards with descriptions, and by category, and any utilities.

The Government Contracting Officer shall approve the transition plan and transition support. At the direction of the government, the outgoing Contractor shall provide input to the government regarding transition activities and work with the incoming Contractor to provide knowledge transfer and transition support, as required by the COR and the Program Manager.

8 DELIVERABLES

The primary deliverable of this task order is deployable application code. The contractor shall deliver this code (in conformance with procedures established by the Integration and Configuration team) throughout the period of performance for integration with an existing codebase in preparation for deployment.

The contractor shall submit electronic copies of document deliverables that are indicated in the table below to the CO and COR (and other cc's as may be specified by the CO and/or COR) via e-mail in the format specified. All document deliverables shall be made by close of business (COB) 4:30pm Eastern Standard Time (EST) time Monday through Friday, unless stated otherwise.

All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.

8.1 Task Order Management Artifacts

The contractor shall provide standard and ad hoc reports that support task order management, as described below:

- Status Briefings

As required by the COR, the contractor shall attend meetings with the COR and/or other USCIS stakeholders in order to review work accomplished, work in progress, plans for future work, transition plans and status, and issues pertinent to the performance of work tasks that require USCIS attention. The meetings may be scheduled regularly or may be ad hoc.

In the event the government requires additional information related to contract technical, cost, or schedule performance, risks, resources, or any contract-related data, the contractor shall provide this report information in the format requested by the government. Requests for ad-hoc reporting may vary in scope and complexity and may require the contractor to attend OIT meetings to obtain required information, review and research applicable documentation, and extract applicable database information required to assemble the ad-hoc report.

8.2 Deliverables Schedule

The deliverables that apply to this task order, and that the contractor shall provide are outlined in *Table 2: Deliverables Schedule*.

Item	Frequency of Delivery	Acceptable Formats
In-process application code (PWS Section 5.2, 5.3 and 5.4)	Continuously, with each build	Application source, GitHub Enterprise markdown code
Shippable application code (PWS Section 5.2, 5.3 and 5.4)	Continuously, with each commit	Application source code and compiled code, GitHub Enterprise markdown
Quality Management Plan (PWS Section 5.5)	30 days after Full Notice To Proceed (NTP) Updated annually	MS Word 2010 or PDF
Product Backlog (PWS Section 5.2, 5.3 and 5.4)	Beginning of each sprint	Electronic / visual board accessible via web (e.g. JIRA)
Reports (PWS Section 5.7)	One business day after each sprint	Demo of product increment, Sprint performance metrics, etc.
Design Deliverables (PWS Section 5.2, 5.3 and 5.4)	End of every applicable sprint	Mock ups and / or design files (if applicable) or design changes reflected in the Development Prototype
Status Briefings, such as presentations, database extractions, meeting reports, burndown charts, etc. (PWS Section 5.7)	As directed	MS Word 2010, Excel, Visio, or PowerPoint
Transition Out Plan (PWS Section 7.2)	30 days prior to expiration of the TO or as directed	MS Word 2010 or PDF
Security Plan (Solicitation Section H)	30 days after Full NTP	MS Word 2010 or PDF
Test Scripts (PWS Section 5.2, 5.3 and 5.4)	Continuously, with each commit	Application source code, GitHub Enterprise markdown, MS Word 2010
Corporate Telework Plan	30 days After Receipt of Order (ARO)	MS Word 2010 or PDF
Separation Notification	Within five (5) days of each occurrence, the CO and COR must be notified of each contract employee termination/resignation. (The COR will then notify the Office of Security & Integrity (OSI) Personnel Security Division (PSD) to coordinate the exit clearance forms.)	MS Word 2010 or PDF
508 Tester List (PWS Section 5)	Quarterly or within 10 days of change in 508 Testers.	MS Word 2010 or PDF

Transition Plan	30 days ARO	MS Word 2010 or PDF
-----------------	-------------	---------------------

Table 2: Deliverables Schedule

8.3 Inspection and Acceptance

Various government stakeholders will inspect contractor services and deliverables. The CO will provide official notification of rejection of deliverables. Inspection and acceptance of deliverables will use the following procedures:

- The government will provide written acceptance, comments, and/or change requests, if any, within 15 days after receipt of task order deliverables.
- Upon receipt of the government comments, the contractor shall, within three (3) business days, rectify the situation and re-submit the contract deliverable(s).

9 TASK ORDER ADMINISTRATION DATA

9.1 Place of Performance

The place of performance will be at the Government-provided work site at 20 Massachusetts Ave, NW Washington, D.C. Up to 50% of teams may be located off-site at a contractor-provided facility. The percentage may increase or decrease at the discretion of the government. This facility may be outside of the National Capital Region (NCR).

The contractor must be located in the continental United States, and must have a central facility available to house teams that are authorized to work outside of the National Capital Region.

9.2 Hours of Operation

Core duty hours for the Government are from 8am to 5pm, Monday through Friday. At times, based on the needs of the mission, the Government will require service outside of the normal duty hours including evenings, holidays and weekends upon COR direction, and given an advanced notice if possible. The outside of normal duty hours' support is expected for production support, outages, releases and potential development. USCIS Government employees must be present during such instances. The contractor shall be available during this time period (see attachment 1).

9.3 Travel

For further guidance, please refer to EAGLE II contract section H.6.1 Travel Costs (Including Foreign Travel).

10 PERFORMANCE CRITERIA

ODOS II contractor teams will be evaluated every 4 weeks using a Balanced Scorecard approach to assess, record, and discuss overall performance. The scorecards will be discussed with the contractor on a monthly basis with the purpose of reinforcing positive behaviors and good performance, and enhancing performance in areas where there are opportunities for improvement. In addition, the monthly scorecards will be used as the basis for past performance reporting in CPARS, and will affect the Contracting Officer's determination to exercise Optional periods and Optional line items.

The objectives for utilizing a Balanced Scorecard approach is to drive continuous performance improvements – to highlight successes made through implementation of best practices and

innovative thinking, while advancing changes to practices and behaviors considered necessary to improve quality, productivity, and value. It is anticipated that ODOS II contractors will be evaluated against the categories listed in Section 11 PERFORMANCE REQUIREMENTS SUMMARY of the PWS. Every 4 weeks the Government will assign a rating for each category based on an assessment of performance for each team from each contractor. The relative weights of these categories will be adjusted by the Government based on its experiences, and will be communicated to the contractors before the start of each evaluation cycle. The Contracting Officer and Contractor will receive a copy of each evaluation. Contractors may provide comments, or responses, to the scorecards to the COR and the Contracting Officer within a week after receipt of the scorecard and ratings.

11 PERFORMANCE REQUIREMENTS SUMMARY

ODOS II contractor teams will be evaluated every 4 weeks using a Balanced Scorecard approach using the six (6) performance categories listed below:

1. **Business Value and User Satisfaction.** Stories and features completed by contractor teams will be evaluated by government Portfolio Manager(s) and Product Owner(s) for the quality and magnitude of business value delivered (inherent in determining satisfaction towards meeting Acceptance Criteria and the Definition of Done), and the degree in which end users are satisfied with the results/outcomes delivered. Evaluations may include feedback from government Product/Project Managers (PMs), Business Advisors (BAs), and Subject Matter Experts (SMEs).
2. **Security, Code Quality, and Architecture/Design.** Contractor code will be evaluated by the Government and Quality Assurance (IV&V) providers against DHS and USCIS security and code quality standards and policy, to include architecture and design guidance and best practices. Continuous/automated code scanning/inspection tools and manual reviews of trouble tickets/incidents will also be used to evaluate code quality.
3. **Test Quality and Test Coverage.** Contractor teams will be evaluated on their ability to write, test, and deliver code that works under all conditions, and meets production quality standards – without reliance on specialized test teams or quality assurance specialists. The contractor will be assessed based on the quality of unit and integration tests delivered within the code, and the extent to which they appropriately test the capabilities and functions. The government will utilize metrics such as escaped defects to determine the extent that code meets production quality standards.
4. **Productivity.** Contractor teams will be assessed based on relative measures of productivity such as speed and efficiency of delivered products and services. The contractor's level of effort compared to the output of work will be evaluated using typical productivity measures, such as a) total story points delivered per sprint (velocity); b) total number of stories a team can reliably deliver per sprint (throughput); c) average length of time it takes to deliver stories from start to finish (cycle time); and d) ability to estimate and predictably deliver completed stories throughout development (flow). The government will be able to compare

across teams to determine relative speed (accelerating, stalling, or regressing), responsiveness to swings in priorities, and to note any unproductive behavior or resistance to change.

5. Collaboration and Innovation. Contractor teams will operate within an ecosystem of federal and contract staff, with multiple teams working in parallel and with constant interaction with USCIS employees. The contractor will be evaluated based on their willingness, effort, and ability to work collaboratively across this ecosystem. Contractor teams will be evaluated based on innovative approaches they introduce to accomplish the work assigned, and their willingness and demonstrated effort to work collaboratively across the entire ecosystem to share knowledge, experience, and lessons learned. The government will evaluate contractors based on examples of innovative approaches that are introduced – whether or not they are self-reported.

6. Process Discipline and Continuous Improvement. Contractor teams will be assessed based on their discipline in implementing Lean software development processes, their conformance to established Agile and DevOps best practices, their contribution to required DHS and USCIS frameworks, their use of retrospectives find more efficient and effective ways to accomplish the work assigned, their use of post mortems to identify and resolve root cause issues, and their ability to demonstrate continuous improvement in areas that can be measured over a time period that spans from a single rating period to several months.

SECTION D – PACKAGING AND MARKING

D.1 Reports and Deliverables

Reports and deliverables provided under this contract(s) shall be provided in accordance with Section C – Performance Work Statement, Section 8.

SECTION E – INSPECTION AND ACCEPTANCE

E.1. FAR Clauses Incorporated by Reference

52.246-4 Inspection of Services -- Fixed-Price (AUG 1996)

52.246-6 Inspection -- Time-and-Material and Labor-Hour (MAY 2001)

E.2. ADDITIONAL INVOICING INSTRUCTIONS

(a) In accordance with FAR Part 32.905, all invoices submitted to USCIS for payment shall include the following:

- (1) Name and address of the contractor.
 - (2) Invoice date and invoice number.
 - (3) Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).
 - (4) Description, quantity, unit of measure, period of performance, unit price, and extended price of supplies delivered or services performed.
 - (5) Shipping and payment terms.
 - (6) Name and address of contractor official to whom payment is to be sent.
 - (7) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
 - (8) Taxpayer Identification Number (TIN).
- (b) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.
- (c) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically to USCISInvoice.Consolidation@ice.dhs.gov with each email conforming to a size limit of 500 KB.
- (d) If a paper invoice is submitted, mail the invoice to:

USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495

SECTION F – DELIVERIES OR PERFORMANCE

F.1 Period of Performance:

Transition Period: 09/30/2018-12/29/2018

Base Period: 12/30/2018 – 03/29/2019

Option Period 1: 03/30/2019 – 09/29/2019

Option Period 2: 09/30/2019 – 03/29/2020

Option Period 3: 03/30/2020 – 09/29/2020

Option Period 4: 09/30/2020 – 09/29/2021

F.3 Deliverables

In accordance with Section 8 of the Statement of Work.

SECTION G – CONTRACT ADMINISTRATION DATA

G.1. EXPECTATION OF CONTRACTOR PERSONNEL

The government expects competent, productive, qualified IT professionals to be assigned to the DevOps teams.

G.2. PERFORMANCE REPORTING

The government intends to record and maintain contractor performance information for this task order in accordance with FAR Subpart 42.15. The contractor is encouraged to enroll at www.cpars.gov so it can participate in this process.

G.3. FINAL PAYMENT

As a condition precedent to final payment, a release discharging the government, its officers, agents and employees of and from all liabilities, obligations, and claims arising out of or under this contract shall be completed. A release of claims will be forwarded to the contractor at the end of each performance period for contractor completion as soon thereafter as practicable.

G.4. GOVERNMENT-FURNISHED PROPERTY

(a) Upon the contractor's request that a contractor employee be granted access to a government automated system and the government's approval of the request, the government will issue the following equipment to that employee by hand receipt:

Equipment	QTY	unit	unit acquisition cost
Laptop computer	1	EA	\$ 4,500
Smartphone	1	EA	\$ 500

(b) The government will issue laptop computers to no more than nine (9) contractor employees per Development Team and to the Management Lead (1) and Technical Leads (2). The government may issue a smartphone to the Management Lead (1) and Technical Leads (2). The equipment will be issued as-is.

G.5. NOTICE TO PROCEED (NTP)

(a) Performance of the work requires unescorted access to government facilities or automated systems, and/or access to sensitive but unclassified information.

(b) The contractor is responsible for submitting packages for employees who will receive favorable Entry-On-Duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. A government decision not to grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such, shall not excuse the contractor from performance of its obligations under these task orders.

(c) The contractor shall submit background investigation packages immediately following task order award(s).

(d) This task order does not provide for direct payment to the contractor for EOD efforts. Work for which direct payment is not provided is a subsidiary obligation of the contractor.

(e) The contracting officer will issue a NTP at least one day before full performance is to begin.

After the transition period a NTP shall not be issued for partial teams.

If needed the additional technical leads shall be included in the NTP for teams #5, 9 and 13.

A NTP will not be issued by the contracting officer until such time as satisfactory suitability determinations have been received and successfully processed by the USCIS Office of Security & Integrity for an entire DevOps Team. The NTP shall specifically identify the Contract Line Item (CLIN) (or sub-Contract Line Item – sub-CLIN) affected. In this manner the government can be clear as to which CLINs or sub-CLINs are able to begin performance. No teams shall be issued a NTP unless the key personnel are available. A NTP may be issued for multiple teams provided all personnel for each team are available.

Regarding staffing, if a request for NTP is submitted prior to close of business on the 15th, or close of business of the last business day prior to the 15th if it falls on a holiday, the NTP shall include the entire month in which the request was made. If a request for NTP is submitted after close of business on the 15th of the month, the NTP shall cite a start date aligning with the next full month.

For those CLINs or sub-CLINs not included in the initial NTP, the duration of their performance periods shall be such that they end at the same time as those started with the initial full performance NTP. Individual CLINs or sub-CLINs shall not have staggered end dates. A NTP issued after the initial full performance NTP shall include the revised performance period per each CLIN or sub-CLIN associated with the NTP.

G.6. POSTING OF CONTRACT (OR ORDER) IN FOIA READING ROOM

(a) The government intends to post the contract (or order) resulting from this solicitation to a public FOIA reading room.

(b) Within 30 days of award, the contractor shall submit a redacted copy of the executed contract (or order) (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA). The contractor shall submit the documents to the USCIS FOIA Office by email at foiaerr.nrc@uscis.dhs.gov with a courtesy copy to the contracting officer.

(c) The USCIS FOIA Office will notify the contractor of any disagreements with the contractor's redactions before public posting of the contract or order in a public FOIA reading room.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 U.S. Citizenship and Immigration Services Office of Security and Integrity–Personnel Security Division

SECURITY REQUIREMENTS

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires that the contractor, subcontractor(s), vendor(s), etc. (herein known as contractor), requires access to sensitive but unclassified information, and that the contractor will adhere to the following.

SUITABILITY DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted contractor employees to government facilities and/or access of contractor employees to sensitive but unclassified information based upon the results of a background investigation. USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No contractor employee shall be allowed unescorted access to a government facility without a favorable EOD decision or suitability determination by the Office of Security & Integrity Personnel Security Division (OSI PSD).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the Position Designation Determination (PDD) for contractor Personnel. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

To the extent the Position Designation Determination form reveals that the contractor will not require access to sensitive but unclassified information or access to USCIS IT systems, OSI PSD may determine that preliminary security screening and or a complete background investigation is not required for performance on this contract.

Completed packages must be submitted to OSI PSD for prospective contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-85P, "Security

Questionnaire for Public Trust Positions” via e-QIP:

1. DHS Form 11000-6, “Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement”
2. FD Form 258, “Fingerprint Card” (2 copies)
3. Form DHS 11000-9, “Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act”
4. Position Designation Determination for Contract Personnel Form
5. Foreign National Relatives or Associates Statement
6. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)
7. ER-856, “Contract Employee Code Sheet”

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified information has resided in the U.S. for three of the past five years, OSI PSD may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

Only U.S. citizens are eligible for employment on contracts requiring access to Department of Homeland Security (DHS) Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer and the Chief Information Officer or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

The contractor must agree that each employee working on this contract will have a Social Security Card issued by the Social Security Administration.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer’s Representative (COR) will advise the contractor that the employee shall not continue to work or to be assigned to work under the contract.

In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years. Security documents will be submitted to OSI PSD within ten business days following notification of a contractor’s reinvestigation requirement.

In support of the overall USCIS mission, contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The contractor shall certify annually, but no

later than December 31st each year, or prior to any accelerated deadlines designated by USCIS, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and contracting officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Insider Threat Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **Unauthorized Disclosure Training** (one time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)

USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-85P security questionnaire.

In accordance with Homeland Security Presidential Directive-12 (HSPD-12) <http://www.dhs.gov/homeland-security-presidential-directive-12> contractor employees who require access to United States Citizenship and Immigration Services (USCIS) facilities and/or utilize USCIS Information Technology (IT) systems, must be issued and maintain a Personal Identity Verification (PIV) card throughout the period of performance on their contract. Government-owned contractor- operated facilities are considered USCIS facilities.

After the Office of Security & Integrity, Personnel Security Division has notified the Contracting Officer's Representative that a favorable entry on duty (EOD) determination has been rendered, contractor employees will need to obtain a PIV card.

For new EODs, contractor employees have [*10 business days unless a different number is inserted*] from their EOD date to comply with HSPD-12. For existing EODs, contractor employees have [*10 business days unless a different number of days is inserted*] from the date this clause is incorporated into the contract to comply with HSPD-12.

Contractor employees who do not have a PIV card must schedule an appointment to have one issued. To schedule an appointment:

<http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/PIV/default.aspx>

Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.

Contractor employees who do not have a PIV card will need to be escorted at all times by a government employee while at a USCIS facility and will not be allowed access to USCIS IT systems.

A contractor employee required to have a PIV card shall:

- Properly display the PIV card above the waist and below the neck with the photo facing out so that it is visible at all times while in a USCIS facility
 - Keep their PIV card current
 - Properly store the PIV card while not in use to prevent against loss or theft
- <http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/SIR/default.aspx>

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

The contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OSI through the COR on all security matters, to include physical, personnel, and protection of all government information and data accessed by the contractor.

The COR and OSI shall have the right to inspect the procedures, methods, and facilities utilized by the contractor in complying with the security requirements under this contract. Should the COR determine that the contractor is not complying with the security requirements of this contract the contractor will be informed in writing by the contracting officer of the proper action to be taken in order to effect compliance with such requirements.

The contractor shall be responsible for all damage or injuries resulting from the acts or omissions of their employees and/or any subcontractor(s) and their employees to include financial responsibility.

SECURITY PROGRAM BACKGROUND

The DHS has established a department wide IT security program based on the following Executive Orders (EO), public laws, and national policy:

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law

93-579, Washington, D.C., July 14, 1987.

- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information*, August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001
- National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004
- DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, *Management of Vital Records*, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only)

Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter. CSAT can be accessed at the following: <http://otcd.uscis.dhs.gov/EDvantage.Default.asp> or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

The USCIS SDLC Manual documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the SDLC manual by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all SDLC activities and deliverables contained in the SDLC. The SDLC is supplemented with information from DHS and USCIS Policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN)*. For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The contractor shall support this process.
- *Risk Assessment (RA)*: This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E.

Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.

- *Certification and Accreditation (C&A)*: This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self-Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

SECURITY ASSURANCES

DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.

- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

DATA SECURITY

SBU systems shall be protected from unauthorized access, modification, and denial of service. The contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and USCIS policies and procedures. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- *Data Labeling*. – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook*.

H.2 DHS ENTERPRISE ARCHITECTURE COMPLIANCE

“All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the government intends to:

- a) All developed solutions and requirements shall be compliant with the Homeland Security Enterprise Architecture (HLS EA).
- b) All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- c) Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

d) Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

e) Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. ”

H.3 CAPITALIZED PROPERTY, PLANT & EQUIPMENT (PP&E) ASSETS INTERNAL USE SOFTWARE (IUS)

Background

The United States Citizenship and Immigration Services Management Directive No. 128-001, USCIS/Office of Information Technology has an ongoing requirement to report Internal Use Software (IUS) costs for the programs under their purview and assignment. This report is a monthly mandatory requirement, and must include all software releases with a cumulative cost of \$500K or greater; bulk purchases of \$1 Million, and a useful life of 2 years or more.

Requirement

Reporting: All applicable charges for application releases and/or development charges are tracked and reported; documented by each applicable release so that an OIT determination can be made if the asset meets IUS criteria. USCIS has determined that the best method for identifying IUS candidates is through monthly collection of contractor cost data for all releases in development, and will capitalize the cost of an IUS project if it is classified as a G-PP&E asset and meets the required criteria.

Definition: IUS is software that is purchased from commercial off-the-shelf (COTS) vendors or ready to use with little or no changes. Internal developed software is developed by employees of USCIS, including new software and existing or purchased software that is modified with or without a contractor's assistance. Contractor-developed software is used to design, program, install, and implement, including new software and the modification of existing or purchased software and related systems, solely to meet the entity's internal or operational needs.

Invoicing and Reporting: The contractor shall identify, capture, log, track and report the costs of IUS associated with each specific release. IUS Software is typically release centric and includes

the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program.

The contractor shall, after OIT's determination on whether or not the release meets the capitalization criteria, support OIT's reporting of costs incurred for the project or release, as required. The contractor shall provide the nature and cost of work completed within the relevant period. Costs considered part of IUS activities include systems administration, systems engineering, and program management. The contractor shall provide the total cost, itemized by release and include the total sum of all applicable IUS activities. At the contractor's discretion, this information may be submitted, either as an attachment or as an itemized line item within the monthly invoices, as outlined in Table 3: Resource Expenditure Format and Figure 1: Resource Expenditure Format. For information purposes, the following activities within the development lifecycle have been identified as IUS reportable costs by the USCIS Management Directive No. 128-001:

a) Design: System Design: Design System, Update System Test Plan, Update Security Test Plan, Update Project Plan, Update Business Case, Conduct Critical Design Review and Issue Memo.

b) Programming/Construction: Establish Development Environment, Create or Modify Programs, Conduct Unit & Integration Testing, Develop Operator's Manual, Update Project Plan, Update Business Case, Migration Turnover/Test Readiness Review, Prepare Turnover Package, Develop Test Plans, Migration Turnover/Issue Test Readiness Memo

c) Testing

i. Acceptance Testing: Develop Security Test Report, Issue Security Certification, Develop System Documentation, Conduct User Acceptance Testing, Update Project Plan, Update Business Case, Conduct Production Readiness Review, Develop Implementation Plan, Issue Production Readiness Review Memo.

ii. Coding

iii. Installation to hardware

iv. Testing, including parallel processing phase

d) Implementation Activities: Implementation/Transition: Security Accreditation (initial system accreditation only), Issue Implementation Notice, Parallel Operations, Update Project Plans, Update Business Case, Conduct Operational Readiness Review, Issue Operational Readiness Memo.

e) In addition, these cost shall contain, if not already itemized in the attachment (PER) or the invoice, the following additional costs information: Full cost (i.e., direct and indirect costs) relating to software development phase; Travel expenses by employees/contractor directly associated with developing software; Documentation Manuals; COTS purchases.

H.4 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) *Applicability.* This clause applies to the contractor, its subcontractors, and contractor employees (hereafter referred to collectively as “contractor”). The contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions.* As used in this clause—

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any government system, contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation
- (6) Criminal History
- (7) Medical Information
- (8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The contractor shall follow all current versions of government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the contracting officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide

- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year) (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how contractors must handle sensitive but unclassified information. DHS uses the term “FOR OFFICIAL USE ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the contractor except as specified in the contract.

(3) All contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA)*, as a condition of access to such information. The contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The contractor shall provide copies of the signed NDA to the Contracting Officer’s Representative (COR) no later than two (2) days after execution of the form.

(4) The contractor’s invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The contractor shall not input, store, process, output, and/or transmit sensitive information within a contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The contractor shall adhere to current government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) *Complete the Security Authorization process*. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) *Security Authorization Process Documentation*. SA documentation shall be developed using the government provided Requirements Traceability Matrix and government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the contracting officer shall incorporate the ATO into the contract as a compliance document. The government's acceptance of the ATO does not alleviate the contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) *Independent Assessment*. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The contractor shall address all deficiencies before submitting the SA package to the government for acceptance.

(iii) *Support the completion of the Privacy Threshold Analysis (PTA) as needed*. As part of the SA process, the contractor may be required to support the government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the government about the use, access, storage, and

maintenance of PII on the contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

(2) *Renewal of ATO*. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The contractor is required to update its SA package as part of the ATO renewal process. The contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the contractor environment to ensure controls are in place.

(3) *Security Review*. The government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The contractor shall afford DHS, the Office of the Inspector General, and other government organizations access to the contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The contractor shall, through the contracting officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the government, for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring*. All contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The plan is updated on an annual basis. The contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or government entities. The government may elect to perform continuous monitoring and IT security scanning of contractor systems from government tools and infrastructure.

(5) *Revocation of ATO*. In the event of a sensitive information incident, the government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the contracting officer may direct the contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The contractor shall provide the government with all information to fully satisfy Federal reporting requirements for contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the contractor shall also notify the contracting officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the contracting officer's email address is not immediately available, the contractor shall contact the contracting officer immediately after reporting the incident to the Headquarters or Component SOC. The contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;
- (xi) Server names where sensitive information resided at the time of the incident, both at the contractor and subcontractor level;
- (xii) Description of the government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and

(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the contracting officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The contractor shall provide full access and cooperation for all activities determined by the government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the government may include, but are not limited to, the following:

- (i) Inspections,
- (ii) Investigations,
- (iii) Forensic reviews, and
- (iv) Data analyses and processing.

(4) The government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements.

(1) The contractor shall have in place procedures and the capability to notify any individual whose PII resided in the contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the contracting officer. The method and content of any notification by the contractor shall be coordinated with, and subject to prior written approval by the contracting officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The contractor shall not proceed with notification unless the contracting officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to government analysis of the incident and the terms of its instructions to the contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the government. Notification may require the contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

- (i) A brief description of the incident;
- (ii) A description of the types of PII and SPII involved;
- (iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
- (iv) Steps individuals may take to protect themselves;
- (v) What the contractor and/or the government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
- (vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements.* In the event that a sensitive information incident involves PII or SPII, the contractor may be required to, as directed by the contracting officer:

- (1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the contractor or resided in the contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the contractor has no affiliation. At a minimum, credit monitoring services shall include:

- (i) Triple credit bureau monitoring;
- (ii) Daily customer service;
- (iii) Alerts provided to the individual for changes and fraud; and
- (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

- (i) A dedicated telephone number to contact customer service within a fixed period;
- (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
- (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
- (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
- (v) Customized FAQs, approved in writing by the contracting officer in coordination with the Headquarters or Component Chief Privacy Officer; and
- (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the contractor shall submit the certification to the COR and the contracting officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

H.5 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user’s responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed

within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

PART II – CONTRACT CLAUSES

SECTION I – CONTRACT CLAUSES

I.1. FAR Clauses Incorporated by Reference

52.204-13 System for Award Management Maintenance (OCT 2016)

52.204-14 Service Contract Reporting Requirements (OCT 2016)

52.209-10 Prohibition on Contracting With Inverted Domestic Corporations (NOV 2015)

52.210-1 Market Research (APR 2011)

52.224-3 Privacy Training Alternate I (JAN 2017)

52.227-14 Rights in Data -- General (MAY 2014)

52.232-7 Payments under Time-and-Materials and Labor-Hour Contracts (AUG 2012)

52.232-39 Unenforceability of Unauthorized Obligations (JUN 2013)

52.237-3 Continuity of Services (JAN 1991)

52.243-7 Notification of Changes (JAN 2017)

52.244-2 Subcontracts (OCT 2010)

(d) ALL

I.2. FAR Clauses in Full Text

52.217-8 Option to Extend Services (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

(End of Clause)

52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The government may extend the term of this contract by written notice to the contractor within 30 days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the government to an extension.

(b) If the government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed thirty-six (36) months

(End of clause)

52.252-2 Clauses Incorporated by Reference (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the contracting officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): <http://www.acquisition.gov/far>

(End of clause)

52.252-6 Authorized Deviations in Clauses (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of this clause.

(b) The use in this solicitation or contract of any Department of Homeland Security Acquisition Regulation (HSAR) (CFR 48, Chapter 30) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of Clause)

I.3. Homeland Security Acquisition Regulation (HSAR) clauses and provisions incorporated by reference.

The full text of HSAR clauses and provisions may be accessed electronically at this internet address: <http://farsite.hill.af.mil/vfhsara.htm>

3052.203-70 Instructions for Contractor Disclosure of Violations (SEP 2012)

3052.205-70 Advertisements, Publicizing Awards, and Release (SEP 2012)

I.4. Homeland Security Acquisition Regulation Clauses & Provisions in Full Text:

3052.204-71 Contractor Employee Access, Alternate I (SEP 2012)

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

- (3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
- (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
- (b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.
- (c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the contracting officer. Upon the contracting officer's request, the contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.
- (d) The contracting officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.
- (e) Work under this contract may involve access to sensitive information. Therefore, the contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the contracting officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.
- (f) The contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, sensitive information, or resources.
- (g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.
- (h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.
- (i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a

right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

- (1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and
- (2) The waiver must be in the best interest of the government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

3052.215-70 Key Personnel or Facilities (DEC 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the contractor shall notify the contracting officer, in writing, before the change becomes effective. The contractor shall submit sufficient information to support the proposed action and to enable the contracting officer to evaluate the potential impact of the change on this contract. The contractor shall not remove or replace personnel or facilities until the contracting officer approves the change.

The Key Personnel or Facilities under this Contract:

Management Lead– EAGLE II Program Manager Level III
Technical Leads– EAGLE II Solutions Architect Level III

(End of clause)

3052.209-72 Organizational Conflict of Interest (JUN 2006)

(a) Determination. The government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting is that an awardee shall not have an Independent Verification and Validation (IV & V) contract or task order supporting USCIS.

(b) If any such conflict of interest is found to exist, the contracting officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract

with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the contracting officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

___ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the contracting officer may require further relevant information from the offeror. The contracting officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the contracting officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divisions that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

PART III – LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.

SECTION J – LIST OF ATTACHMENTS

J.6. Management Instruction for Applying Lean-Agile-DevOps Principles at USCIS – Attachment 6 (14 pages)

J.7. Appendix A: Generally Accepted Agency Practices – Attachment 7 (15 pages)

J.8. Management Instruction for Agile Independent Verification and Validation (IV&V) – Attachment 8 (18 pages)

J.9. Definitions and Clarifications (1 page)



**U.S. Citizenship
and Immigration
Services**

USCIS

Management Instruction for Applying Lean-Agile-DevOps Principles at USCIS

Management Instruction: CIS-OIT-003

April 2017

Unclassified

Version 1.0

ITDL Number: 210950

This document was prepared for authorized distribution only.

This page left intentionally blank.

Office of Information Technology

Management Instruction for Applying Lean-Agile-DevOps Principles at USCIS

Effective Date: 1 May 2017

Management Instruction: CIS-OIT-003

I. Purpose

This Management Instruction (MI) establishes the United States Citizenship and Immigration Services (USCIS) policies, procedures, requirements, and responsibilities for the use of Lean Thinking, Agile Development, and DevOps capability. It supersedes MI CIS-OIT-001 (Agile Development) and MI CIS-OIT-002 (Team-Managed Deployment Onboarding) and should be considered the current guidance for delivering Information Technology (IT) solutions within USCIS.

Lean, Agile, and DevOps methods enable the delivery of fit-for-purpose IT solutions with very short lead times, as measured from identification of a mission need to the delivery of IT capabilities meeting that need. These methods have been shown to produce IT solutions that:

- Satisfy customers
- Maintain ongoing operational capabilities
- Are high quality, thoroughly tested, and technically excellent
- Rapidly adapt even in an uncertain operating environment
- Continuously improve time-to-mission-value

This MI increases emphasis on DevOps thinking to improve USCIS IT service delivery agility and increase the business value of IT projects. DevOps strategies should be used to deploy software more frequently and reliably, act faster on feedback from system operations, and establish a culture of continuous experimentation and learning. These methods have been shown to:

- Enhance quality, reliability, and security of products and services over the long term
- Decrease business risk by lowering change failure rates and system downtime
- Improve outcomes and experiences for system stakeholders, developers, operations engineers, and end users
- Reduce total investment costs

Lean, Agile, and DevOps methods are consistent with the Department of Homeland Security (DHS) Acquisition Management Directive (MD) 102 and the DHS Systems System Engineering Lifecycle (SEL), the Digital Services Playbook, "Modular First" guidance from the DHS Chief Information Officer (CIO), the Federal Chief Information Officer's 25 Point Implementation Plan, and the Office of Management and

Attachment 6 - Applying Lean-Agile-DevOps Principles at USCIS

Budget (OMB) Modular Contracting Guidance. The "modular and incremental" approach encouraged in these documents mandates that the government continuously learn and improve at delivering low cost, low risk IT solutions. In order to monitor these outcomes, this MI includes governance designed to provide rich, ongoing visibility into USCIS system development, delivery, and operations.

II. Scope

This MI applies to all employee and contractor teams involved in the planning, development, and deployment of software and systems throughout USCIS.

III. Authorities

The following laws, regulations, orders, policies, directives, and guidance authorize and govern this Management Instruction:

1. DHS MD 102-01 Acquisition Management Directive, and associated Instructions and Guidebooks
2. Section 5202 of the Clinger-Cohen Act of 1996
3. OMB Circulars A-130 and A-11
4. 25 Point Implementation Plan to Reform Federal Information Technology Management (U.S. Chief Information Officer, December 9, 2010)
5. Contracting Guidance to Support Modular Development (OMB, June 14, 2012)
6. Memorandum on Agile Development Framework for DHS, by DHS CIO, Richard A. Spires, issued June 1, 2012
7. Digital Services Playbook (<https://playbook.cio.gov>)

IV. Policy, Procedures, and Requirements

Except in cases where a waiver is granted by the USCIS CIO, all systems development and maintenance projects at USCIS will follow this Lean-Agile-DevOps MI. Such projects include custom software development, Commercial Off-The-Shelf-Software (COTS) integration and configuration, business intelligence, and reporting capabilities. Where appropriate, Lean-Agile-DevOps approaches may be used for other IT and non-IT projects. For the purposes of this MI, projects will be considered in compliance if they achieve the outcomes specified in Sections A and B. To achieve these outcomes, teams and programs may elect to use practices from the set of Generally Accepted Agile Practices listed in the Appendix and work with Independent Validation & Verification (IV&V) teams to ensure that they fulfill the MI CIS-OIT-004 (Agile Independent Verification and Validation).

USCIS Office of Information Technology (OIT) management will ensure that appropriate training, coaching, and tools are available to facilitate the success of all projects. Teams are encouraged to work with OIT support groups to implement this MI in a manner appropriate for their particular context.

Attachment 6 - Applying Lean-Agile-DevOps Principles at USCIS

A. Lean-Agile and DevOps Approaches Defined

Lean can be characterized as "the art of maximizing work not did" by increasing flow and reducing waste. Leanness is measured for IT projects by the lead time from identification of a need to the time a corresponding capability is delivered. Waste is defined as work that does not add enough value to justify itself, such as handoffs, delays, and unnecessary intermediate work products. Lean IT projects at USCIS continuously improve efficiency and responsiveness to mission needs on behalf of the public.

Agile approaches use an iterative, incremental, and collaborative process to deliver small, frequent software releases. Effective agile methods yield rich information from tight feedback loops, providing customers and delivery team's frequent opportunities to adapt based on changing project conditions. A number of agile methods are in common use at USCIS, including Kanban, Scrum, and Extreme Programming (XP). The values common to agile practices are articulated in the Agile Manifesto, which elevates interaction, working software, customer collaboration, and responding to change. The intent of the agile values is not to prescribe a set of mechanical steps or ceremonies but to guide an empirical, feedback-oriented agile mindset. Teams that follow agile values are likely to benefit from the "guardrails" inherent in the agile approach. Teams are encouraged to use practices from one or more agile methods as appropriate and to incorporate innovations from the agile community.

DevOps approaches subscribe to a seamless collaboration of operations and development engineers to fulfill business needs through delivery of stable, secure, and reliable services to customers. DevOps methods yield timely feedback at all points in the service lifecycle, improving the ability to reliably deploy software, respond to feedback from production operations, and continuously improve quality. A number of DevOps strategies are commonly used at USCIS, including Continuous Integration, Continuous Deployment and Continuous Operations.

B. Required Outcomes

USCIS develops IT solutions to support the mission of the agency. In order to achieve the desired impact, we require certain outcomes from software development, deployment, and operations processes. Where required outcomes are difficult to measure directly, measurement and observation can be used to infer them. These observations are guided by asking key questions to assess whether the desired outcome is being achieved.

The key questions presented for each outcome in this MI are not a definitive list. Programs should determine effective outcome measurements in their own context and track the trends of those measurements. Programs are also expected to change the questions and measurements over time to ensure they are checking the most important concerns. In addition to self-assessment, programs should coordinate with USCIS Independent Verification and Validation (IV&V) to assess effectiveness, facilitate transparency and accountability, and provide feedback to teams and management from an independent viewpoint.

Outcome #1: Programs and projects frequently deliver valuable product

Earlier delivery allows earlier accrual of value. Earlier use provides feedback on suitability.

Key Questions

- How frequently is the working system delivered to stakeholders for review?
- How frequently is the working functionality delivered to end users for use?
- What is the cycle time (mean, distribution) from start of work on a feature to delivery?
- What is the lead time from ideation/approval to use?
- How do you verify that the systems you're developing are solving the intended problem? How quickly do you know?

Outcome #2: Value is continuously discovered and aligned to mission

Teams and their business partners continuously discover emerging needs for their products. Delivered capability can and should trigger new discoveries.

Key Questions

- What business outcomes or strategic objectives are supported by the work being done?
- How do you know that you're working on today's highest priority items?
- What is the customer (stakeholders, users) satisfaction with delivered functionality?
- What actionable insights from end users are addressed over time?
- What is the team satisfaction with business engagement and direction?
- How can the value delivered be measured (understanding that sometimes a quantitative measure is not appropriate or feasible)?

Outcome #3: Work flows in small batches and is validated

Batch deployments significantly reduce risks associated with deployment. Low risk deployments promote flow of new capabilities to production.

Key Questions

- How is daily progress toward goals made visible? Is it a reliable progress indicator or does it hide surprises?
- Is work in progress finished before new work is started?
- How completely is incremental work validated before it is considered done?

Outcome #4: Quality is built in

Work processes address quality as a matter of course rather than as remediation. Avoiding problems provides more benefit than solving problems.

Key Questions

- What is the demand for remedial work?
- What is the incident rate of escaped defects?
- Are your tests automated and structured to provide the quickest feedback (unit tests)?
- Are you testing at all layers of the application with appropriate investment (test pyramid)?
- How easily does the system architecture and design allow for modification and extension?
- What precautions have been taken to reduce consequences when there is a system failure?
- What measures are in place to monitor the intrinsic quality of the code?
- How frequently do commits fail in the build/test/deploy pipeline?
- Does the system meet appropriate performance thresholds? As the system is modified, what are the trends in performance measurements?

Outcome #5: The organization continuously learns and improves

Improvements come from increased knowledge and skill. Performing the work provides deeper insights into improved methods.

Key Questions

- How freely can teams innovate and improve daily work?
- How inclusive is the collection of improvement ideas?
- How safe is it to try experiments that may not lead to expected results?

Outcome #6: Teams collaborate across groups and roles to improve flow and remove delays

The desired result is more than the sum of individual roles. Overlap is needed to prevent gaps between business and technical roles. Handoffs result in lost information and delays. Much important knowledge is tacit, and can best be shared by working together.

Key Questions

- How much code is reused across teams?
- What diverse roles explore the details of the requirements and what are the indicators of satisfaction of the requirements?
- What indications are there of responsibilities being shared across groups?
- How much time is spent waiting for another team's work?

Outcome #7: Security, accessibility and other compliance constraints are embedded and verifiable

Systems must not only have to work correctly for intended use, but also resist unintended abuse. In addition, there are mandates in law and executive direction that must be followed. Notable among these are disability accessibility and privacy protection. There are also constraints about the language used to communicate with the public.

Key Questions

- How are security, accessibility, and organizational constraints communicated throughout the project community? What indications are there that these constraints are well understood?
- Are security, accessibility and privacy requirements treated the same as functional requirements? How are they addressed in the requirements process? Are they prioritized as highly?
- How are security, accessibility and privacy addressed in system design and code structure?
- To what extent are security testing and controls integrated into daily work? How much is automated? How early does it detect issues?
- How is compliance with all security requirements verified in an ongoing manner and documented with auditable evidence?
- How is Section 508 Compliance verified as the system is developed and documented with auditable evidence? What controls are in place to notice undesirable changes or other actions made by an individual? How do we confirm and provide evidence that controls are operating effectively?

Outcome #8: Consistent and repeatable processes are used across build, deploy, and test

Consistency is required to maintain quality across delivery. Teams who have an understood and repeatable process can gauge the efficacy of the improvements made.

Key Questions

- How many manual steps are there in the current build, deploy, and test process, and what is the team doing to reduce that number?
- Is there a common code repository/branch that is built, tested, and deployed on every commit?
- How long does code exist on other branches or the developer's machine before merging to the common code?
- What degree of confidence does the suite of automated tests provide?
- How quickly and easily can build failures be resolved?

Outcome #9: The entire system is deployable at any time to any environment

Unfinished work in progress provides no benefit and may block the efforts of others. The system should be maintained in a working state even as modifications are being made.

Key Questions

- Can the same automated script deploy to every environment?
- Are database changes and rollbacks automated with version-controlled scripts?
- To what extent is the setup and configuration of environments automated with version-controlled scripts?
- To what extent is the build/deployment pipeline automated with version-controlled scripts?
- How long does it take to stand up a complete test environment with production or production-like data?

Outcome #10: The system has high reliability, availability, and serviceability

Attention must be focused on the robustness of the system in the face of errors, the ability to be used as development proceeds, and the ability to quickly detect and correct latent problems.

Key Questions

- Can various parts of the system be built and deployed independently?
- To what degree is the system meeting the reliability, availability, and serviceability needs of the mission?
- How long does it take to detect, ameliorate, and correct operational problems?
- Are the operational characteristics of the system being validated in production through monitoring, reporting, and alerting? How?
- Is the system designed in such a way as to be cost-effective in operation?

V. Generally Accepted Agency Practices

Each program or project chooses a baseline set of practices that support the Lean-Agile-DevOps outcomes listed in this document. The chosen practices should be documented in the Team Process Agreement (TPA) and improved over time. The program or project may solicit an independent assessment of its practices following the USCIS IV&V Policy and will be expected to justify its practices to the RPR Authority (USCIS CIO or designee). Improvements that are material should be documented by updating the Team Process Agreement (TPA) before the next RPR and the program or project should be able to justify its TPA practices if questioned about them in the RPR.

MI CIS-OIT-003 Appendix A lists typical agency practices, derived from Agile and DevOps methods commonly followed in the software development industry. Nothing in this document should be construed as prohibiting even better practice, but is intended to guard against insufficient discipline or governance. Practices may be reviewed by the CIO or designee at any time, particularly in the RPR, or on the advice of Quality Assurance, and the program or project should be able to justify the chosen practices.

VI. Governance

The purpose of this governance is to ensure the government's interest in delivering appropriate IT solutions on behalf of the public. Governance responsibilities include:

- Ensuring changes to IT systems pose appropriately low risk to mission fulfillment
- Managing alignment with the overall strategic direction of mission
- Providing transparency to project stakeholders and opportunities for involvement by those impacted by system changes, including end users
- Verifying projects are carried out with appropriate procurement, contracting, and hiring practices in order to meet fiduciary constraints
- Continuously improving governance and oversight mechanisms to ensure that they accomplish project goals in a lean manner

This MI represents a tailoring of the SELC included in the annexes to DHS acquisition guidance presented in DHS D-102. Appendix B provides the tailoring plan that demonstrates this alignment with D-102. By following this MI, USCIS Lean-Agile-DevOps projects will maintain compliance with D-102. Programs on the DHS Major Acquisitions Oversight List will, in addition, need to fulfill the requirements of the D-102 Acquisition Lifecycle Framework (ALF).

Attachment 6 - Applying Lean-Agile-DevOps Principles at USCIS

A separate MI, CIS-OIT-004, describes the USCIS Agile Independent Verification and Validation USCIS Independent Verification and Validation (IV&V) approach that will be used to evaluate adherence to this MI and will inform governance activities.

During the “Obtain” phase of the program acquisition lifecycle, system development activities will proceed through a number of increments, or release cycles. For each increment, the following gate reviews will be held:

Lean Release Planning Review (Lean RPR)

Lean Release Planning is the means by which USCIS agile projects establish time, cost, and a notional plan for delivering new capabilities. Lean Release Planning artifacts should include minimum documentation necessary to effectively communicate release plans and should be published in a location accessible to all stakeholders. Once a minimum set of artifacts is established at the outset of a project, artifacts should be updated incrementally throughout the release cycle to reflect current reality.

The RPR Meeting is a gathering of stakeholders to review release plans and align resources to support them. The RPR Authority (USCIS CIO or designee) will assess a project's readiness to proceed with a time boxed release cycle of no more than six months. A business decision will be made as to whether the investment in the release cycle is justified by the expected results (capabilities to be produced). The project may not proceed to release activities (development, testing, etc.) until it has secured RPR approval.

The RPR Authority will assess the project's likelihood of achieving the outcomes required by this MI (sections A and B). The RPR Authority will review appropriateness of resourcing and skill levels, agile team processes, technical practices, the team's understanding of capabilities to be developed, oversight and transparency mechanisms, and dependencies on other projects and infrastructure. The project will demonstrate its readiness through thoughtful discussion with the RPR Authority, by providing evidence that stakeholders and delivery team members concur with release plans, and by producing a set of Lean RPR artifacts.

Core RPR Artifacts:

- Capabilities and Constraints (CAC)
- Project Oversight Plan (POP)
- Team Process Agreement (TPA)
- Release Characteristics List

Other artifacts, such as Section 508 Compliance Determination Forms (CDF), may be required depending on the specific project, which will be established by agreement with the RPR Authority.

Attachment 6 - Applying Lean-Agile-DevOps Principles at USCIS

Team-Managed Deployment (TMD) Onboarding

TMD Onboarding is an IV&V process to validate a system's capability to operate with high reliability, availability, and serviceability using robust automated build, test, and deployment practices. Systems should be on boarded to TMD when they satisfy outcomes 7, 8, 9, and 10 in this MI. Following TMD onboarding, RPR approval constitutes authorization for teams to deploy directly to production for up to six months. To minimize risk, teams are encouraged to deploy as often as multiple times per day, and must deploy to production at least every two weeks.

TMD requires ongoing communication and collaboration of development engineers, operations engineers, and business stakeholders. The following team agreements are required to facilitate effective teaming across the project community.

1. *Product Owner Acceptance* – The Product Owner retains full authority and responsibility for approving features deployed both through feature toggles and by direct code push to production. Teams are strongly encouraged to make this Product Owner approval a step in the continuous delivery pipeline.
2. *Communications Agreements* – Teams make agreements with key stakeholders regarding notifications before, during, and after deployment. Stakeholders include the user community, operations support engineers; help desk personnel, the Information System Security Officer (ISSO), Quality Assurance, and other impacted groups. Teams are encouraged to provide notifications via an Operations Monitoring Dashboard.
3. *Monitoring* – Teams prepare an Operations Monitoring Plan or Dashboard showing the practices, tools, and measures that will monitor applications in production. The plan will include an operations review schedule and escalation procedure when monitoring thresholds are breached. In lieu of a document, an Operations Monitoring Dashboard is the preferred long-term approach.
4. *Documentation* – Teams regularly and appropriately update the document set in accordance with their Program Oversight Plan (POP). Artifacts requiring regular updates may include a Pipeline Design Document, System Design Document or Wiki (SDD/W), Interface Control Agreements (ICAs), and Section 508 and Security Documentation. Teams are encouraged to use agile documentation approaches such as self-documenting code and tests expressed in a business-friendly language. Agreements regarding such approaches should be noted in the POP.
5. *Periodic Audits* – Teams make agreements for periodic audits of 508 compliance, security compliance, and other auditing oversight deemed necessary during the RPR.

USCIS OIT Applied Technology Division (ATD) will support the team in this effort by providing an independent assessment on pipeline suitability for TMD Onboarding. TMD is encouraged for all USCIS teams but granted on a contingent basis--provided the system remains in compliance.

Attachment 6 - Applying Lean-Agile-DevOps Principles at USCIS

Release Readiness Review for TMD Systems (TMD-RRR)

RRRs for TMD systems will be held periodically to approve the release of major new functionality to users through a deployment or feature toggle. The criteria and/or schedule for holding TMD-RRRs for a particular system will be determined according to risk, using the risk model described in the USCIS IV&V Policy, and will be documented in the system's TPA. RRRs may also be held on demand by the CIO and on the advice of Quality Assurance, based on risk.

Legacy Release Readiness Review (RRR) and Electronic Release Readiness Review (eRRR)

Systems without TMD approval must hold a Release Readiness Review prior to each production deployment unless a waiver is granted by the Delivery Assurance Branch. An RRR may be conducted as a meeting or, per agreement with the RRR Authority, as a sequence of electronic approvals. In order to assess whether the current increment is ready to be deployed, the RRR Authority will assess whether the deployment was adequately tested, reviewed by the product owner and users, and is compliant with enterprise architecture, coding standards, Section 508, and security requirements. The RRR Authority also verifies that release activities were coordinated with business stakeholders and that the business is prepared for the impact of the release. Finally, the RRR Authority assesses the deployment and rollback plans and ensures the deployment package is ready to be submitted to applicable change control boards (CCBs). If the RRR Authority approves the release, it is then submitted to Change Control and deployed.

Core Deployment Artifacts (TMD-RRR, RRR, and eRRR):

- System Design Document or Wiki (SDD/W)
- Automated and Manual Build and Installation Scripts
- Automated and Manual Test Scripts
- Automated and Manual Deployment Scripts
- ICCB or Change Control Board Package
- Security Plan (SP)
- Security Assessment Report (SAR)

Other artifacts, such as Section 508 Compliance Determination Forms (CDF), may be required depending on the specific project, to be established by agreement with the RRR Authority.

Post Implementation Review (PIR) / Release Cycle End

During the PIR, the PIR Authority (USCIS CIO or designee) and the team will analyze the project's successes and failures during the release cycle to identify improvements to the next release cycle. The review will include the Product Owner's assessment of the business value generated during the release cycle, software quality measurements, Section 508 compliance, security compliance, and POAM resolution. The PIR also constitutes the formal end of a release for IUS purposes. The primary focus of the PIR, though, is to celebrate value that was delivered and identify continuous improvement

Attachment 6 - Applying Lean-Agile-DevOps Principles at USCIS

opportunities. Teams should work with USCIS IV&V teams to provide an independent assessment of key measurements and outcomes of the release. Teams are encouraged to hold the PIR in conjunction with the RPR meeting for the next release cycle.

Additional Procedures

Lean-Agile-DevOps projects must conform to the USCIS policy IV&V in order to:

- Provide transparency and accountability to the public
- Inform management and oversight bodies with an independent view of what is working or not working in program execution, based on data and analysis
- Provide feedback to program executors to help them improve their processes

VII. Questions, Comments, and Suggestions

Please address any questions, comments, or suggestions to: USCIS-QA-TEAM@uscis.dhs.gov

VIII. Approval

Signed: M. A. Schwartz

Date: 4/25/2017



**U.S. Citizenship
and Immigration
Services**

USCIS

**Appendix A: Generally Accepted Agency
Practices**

**Addendum to MI CIS-OIT-003 Management
Instructions for Applying Lean-Agile-DevOps
Principles at USCIS**

March 2017

Unclassified

Version 1.0

ITDL Number: 210951

This document was prepared for authorized distribution only.

This page left intentionally blank.

Office of Information Technology

Addendum to MI CIS-OIT-003 Management Instructions for Applying Lean-Agile-DevOps Principles

Effective Date: 1 April 2017

Management Instruction CIS-OIT-003 Appendix

Appendix A. Generally Accepted Agency Practices

In pursuit of the Required Outcomes called out in CIS OIT Management Instruction CIS-OIT-003, the following generally accepted practices may be used to achieve successful software development. The Key Questions for each Required Outcome help identify and measure areas of improvement. Table 1 depicts the outcomes supported by each of the practices.

Teams planning to practice Team Managed Deployment (TMD) are expected to have a higher level of Agile discipline than the minimal guidelines.

The team-chosen enabling practices commonly include the following:

Delivery Cadence

The development teams deliver incremental improvements to the agency on a regular and frequent basis.

These deliveries of working functionality allow the work completed so far to be experienced, providing an unambiguous indicator of progress and a potential discovery of previously unknown needs.

- Deliver to production no less frequently than *quarterly*
- For TMD, deliver to production no less frequently than the *development cadence*, and potentially *multiple times per day*

Delivery Environment

Development delivery must be able to provide value to the agency, either to allow stakeholders to experience the current system capabilities and limitations, or to end users for actual use.

- At minimum, to an internal environment where stakeholder can examine and evaluate the system
- Customarily to an environment that mimics production
- For TMD, to production use

Iterative, Incremental Development

Development should proceed in small slices of functionality. As development proceeds, existing functionality should be revisited to add additional or modify existing functionality (iterative). New or modified functionality should extend existing working functionality, leaving the whole in a working state (incremental).

- Development cadence of no longer than *4 weeks*
- For TMD, development cadence no longer than *2 weeks*
- Short enough for effectively steering the project
- Small increments of functionality are validated as they are developed
- Projects shall use time boxes or limited work in progress (WIP) policies to enforce short cadences for planning, completing, demonstrating, and deploying working tested features
- For TMD, validation of accumulated functionality is continually validated, mostly with automated checks, to enable development flow without regressions

Embedded Product Ownership

The direction of development, what functionality should be developed and in what order, should be embedded with the development team, authorized and available to make decisions as needed without delay.

- The Agency needs are represented by a single clear voice to development, dedicated to the development effort
- Product Owner has full authority to make timely decisions regarding development, prioritization, and acceptance of development
- Product Owner has full authority to make decisions about when functionality is deployed either by turning on a feature toggle or by direct code push to production
- Close collaboration between dedicated representative and actual stakeholders and users
- Teams are encouraged to include Product Owner approval as part of the continuous delivery pipeline
- For TMD, frequent feedback of the developing system from the actual stakeholders and users, informing future development, priorities, and fitness for purpose

Representation of Requirements

The documentation of requirements for development should be tuned to the needs of the development process and regarded as ephemeral. Any need to document beyond the development process should be regarded as separate and designed to meet that need.

- Explicit conditions of satisfaction that may be validated
 - Acceptance criteria describing the intent
 - Acceptance scenarios illustrating essential cases

- Use of low over-head, low fidelity assets such as user stories, augmented as needed with elaborations such as paper prototypes, or sample reports to convey the essential behavior
- Independent pieces capable of being sequenced in almost any order
- Small enough to easily fit within the delivery cadence

Automated Testing

In keeping with “test early, test often” principles, test criteria defined early in the life of a user story drives creation of automated test code that is stored in the version control system along with all other code. Automated tests should include appropriate testing such as unit testing, functionality, and system-to-system interfaces. While complete automated testing is desired, security and Section 508 accessibility testing will be automated when tools are available to support. Risk-based approaches should be used to determine which automated tests are included in regression suites.

- The explicit conditions of satisfaction determined in the requirements are automated as acceptance tests
- Functionality is typically tested over the smallest scope possible, and includes edge conditions
 - The Agile Testing Pyramid may be used to visualize this
- For TMD, high level of reliable automated testing
- For TMD, performance measures are tracked over time by the development teams

Fail-Safe

Concern should be paid to execution that may not proceed as desired and what consequences this will have. Negative consequences should be minimized and recovery procedures should be considered.

- System design shall anticipate environmental and implementation failures and mitigate the consequences
 - This may be monitored by the consequences and time-to-fix for production incidents
- For TMD, tests are treated as valuable as code, and gaps or failures are treated as first-class issues
- For TMD, perform as many infrastructure tasks as possible programmatically
- For TMD, it should be feasible to revert to the previous version, including database schema or data changes and environment
- In close coordination with operations engineers, development teams implement and test methods to monitor, minimize, and correct unanticipated issues associated with deployments. Preferably, these methods are automated. These methods may include blue/green deployments, feature toggles, rollback scripts, and “fail forward” approaches that enable rapid replacement of faulty elements. Recovery methods

should be executed quickly to minimize impact to data, system performance, and other critical aspects of production applications.

Extrinsic Quality

Care should be taken to keep the external quality of the system, as seen by the users, sufficiently high at all times to give correct operation and ease of use.

- Every feature is specified with one or more essential tests representing the intended functionality
- External expertise is engaged for extended verifications (e.g., security, accessibility) on a regular basis
- Testing activities happen within development cadence
- Testing capabilities are embedded within the teams

Intrinsic Quality

Care should be taken to keep the internal quality of the system, as seen by the developers, sufficiently high at all times to promote ease of development, understanding, and modification.

- System implementation shall not impede the addition or modification of functionality
- This may be measured in arrears by counting the number of modules that must be modified for a change
- As units of code are created, they are simultaneously tested for proper operation, resilience to unexpected inputs, and boundary conditions
- Unit tests document the code behavior intended by the programmer and verify that the code exhibits this behavior

Emergent Design

The design of the system should be envisioned and realized over time.

The more we work on the system, the better we understand the needs of the mission and the needs of the implementation context.

At any given time, the system design must support current functionality without being overdesigned to support future functionality.

Anticipated future needs of the system should be designed as needed.

Care should be taken to keep such needs in mind so that they may be feasibly implemented when the time comes.

Such an approach not only maximizes the realized benefit of the design, but leaves the agency best prepared for future changes in mission needs.

- Avoid building unused "hooks" anticipating future needs
- Keep the design simple so that future needs are easy to accommodate as they arise

Refactoring

As the needs of the design shift, it's often necessary to modify existing code without changing its functionality.

This process is called Refactoring, a term attributed to William Opdyke and Ralph Johnson after their September 1990 article on the topic. The best known reference to this technique is Martin Fowler's book, *Refactoring. Improving the Design of Existing Code*.

By reshaping code without changing its functionality, we can correct deficiencies we discover in our design or make the design amenable to new demands we place on it.

- Separate changes in code structure from changes in code functionality
- Use well-known refactoring techniques that are known to preserve functionality
- Make restructuring changes as a series of small changes, keeping the code functional at each step

Intentional Architecture

Make design decisions intentionally, rather than through expedience. Anticipate technical risks and design the architecture to meet them as they are addressed.

- Keep an eye on the long-term goals and technical issues as the design emerges
- Communicate the issues and current thinking on architectural approaches to all members of the development team
- Listen to any questions or objections concerning the suitability of the design

Managing Technical Debt

Ward Cunningham invented the term *Technical Debt* to describe the difference between how we currently understand the problem domain and how it is represented in our code. This difference naturally creates difficulties as we expand our coverage of the problem domain.

For example, we might model a domain construct as a hierarchical tree, but later find that some nodes are referred by more than one node. Our tree implementation cannot model that. Refactoring the code to a directed acyclic graph implementation will model our current understanding of the problem domain more directly.

Since then, others have come to use the phrase *Technical Debt* any perceived deficiency in the code design.

Whether using a strict or loose definition, it's important to manage these deficiencies so that the code does not become difficult to maintain and extend.

- Keep duplication of functionality at a minimum
- Write code that expresses the concepts on the mind of the programmer, such that they are obvious to the next person to touch this code
- In object-oriented code, follow Robert C. "Uncle Bob" Martin's SOLID design principles
- In all code, maximize cohesiveness of any module or grouping, and minimize its coupling to other modules or groupings

Version Control

Teams frequently commit working code to a USCIS-owned repository using an automated mechanism. In this context, code implies all system source code, configuration files, automated test scripts, build scripts, deployment scripts, or other computer files needed to build the system or the supporting Continuous Delivery pipeline.

- All code is version-controlled
- Developers and teams should integrate their code frequently
 - Code is merged into common branch more frequently than development cadence
 - Code from the common branch is frequently merged into each developer's working copy, preferably multiple times a day
- Minimal time between introducing a change and other teams accounting for that change
 - For TMD, multiple times a day
- Documented procedures for build, test and deploy are version-controlled with the code
- It shall be feasible to retrieve and build any previous version, preferably by name, date or tag
- It shall be feasible to see the history of changes and to compare any two versions

Scripted Builds

Build processes should be well-defined so that they are repeatable as a matter of course.

- Build processes are scripted to allow anyone to build any portion of the system in a repeatable manner
- Build scripts should be version-controlled with the code
- Build scripts should contain segregated build steps for compiling, unit testing, producing deployable artifacts, and other desirable units of work

Automated Builds

To the extent feasible, build processes should not rely on manual intervention for execution. Human intervention should be reserved for decision making.

- Builds are performed via automated, script-driven retrieval of source code from a repository monitored by a dedicated build server
- Builds should run on code check in, on a set frequency, on demand, or any combination of these
- Builds should run a sequence of build scripts to compile, unit test, and produce deployable artifacts. Builds may automatically deploy artifacts and test them in situ
- Builds should complete within a short duration

- The build server should produce appropriate build notifications and always present build status

Scripted Deployment

Deployment procedures should be well-defined so that they are repeatable as a matter of course.

- The same documented procedures are used to deploy to any environment, including Production
- For TMD, these procedures should be scripted and version-controlled

Deployment with minimal downtime for users

- Small releases
- Decoupled services
- Zero downtime (e.g., blue-green) deployments
- Database migration scripts
- Forward and backward compatibility of components
- Backout capability

Automated Deployment

To the extent possible, deployment scripts should not rely on manual intervention for execution.

- Teams maintain an automated process (or set of processes) that executes a list of deployment steps via script or via a deployment tool
- Automated deployments should be rapid, reliable, testable, and repeatable
- Steps include running acceptance tests, pushing code to downstream environments, and automated smoke testing
- Communication artifacts, such as tickets and release notes, should also be automatically generated. Deployment configuration scripts should be stored as code and placed under configuration management

Approved Pipeline

The components and procedures to build, test and deploy software should be reliable and trusted.

- Teams implement a Continuous Delivery pipeline approved by USCIS.
 - Pipeline components may already be in use at USCIS or, per agreement, may be emerging tools in the market that are new to USCIS
- For TMD, procedures for build, test and deploy are automated

System Monitoring

Systems should be monitored in production to detect problems in a timely fashion for quick action, and to provide the business with information about normal use.

- Teams shall have procedures and tools in place to monitor the performance and health of the system in production
- Key elements should be displayed in a dashboard viewable at any time
- Automated systems may monitor that operations are within defined thresholds
 - Appropriate personnel should be alerted when thresholds are breached
 - Incident management and escalation procedures should be defined

Release Planning

Planning for future releases should provide guidance to external stakeholders while providing flexibility for the appropriate definition and delivery of system details.

- Adaptive Rolling Wave Planning to maintain a clear vision of immediate capability delivery in the context of a longer range view

Visibility of progress

The progress being made toward program goals should be easily visible and reflect the current reality.

- Visibility into team's progress toward program goals (e.g., burn-up)
- Practices in place for communication and collaboration across teams (e.g., Scrum of Scrums, Portfolio Alignment Wall)

Peer reviews

Avoid single points of failure by collaborating with others, filling in knowledge gaps, catching oversights, and considering a diverse set of options.

- Peers should review each other's code, tests, and other development artifacts
- Reviews should attempt to identify system risks not caught by tests and automated analysis
- Reviews should share information and development styles across the development team

Integrated Experimentation & Learning

In recognition that the beginning of a program is the point in time at which the least is known about it, experimentation and learning should be conducted to maximize improvement as development proceeds.

- Regular team retrospectives at development cadence with tangible results

- Periodic program retrospectives over larger intervals and participants
- Capacity is allocated for experiments and improvements as a normal part of development

Culture of learning

In recognition that the majority of the time and effort in a program is spent learning what and how to do things, institutionalize learning as a major part of the program execution.

- Outside the development process, institute periodic sharing of technical and process learning
 - Communities of Practice, Guilds, Brown Bags

Deployment History and Consistency

Place the highest value on meeting needs through the life of the program, demonstrating trustworthiness.

- Teams should demonstrate a record of successful deployments
 - Success measures include avoidance of emergency conditions and post-release issues
 - Should a problem occur as an aberration, teams should demonstrate an ability to eliminate the root cause, ensuring a one-time issue does not become a pattern of dysfunction

Table 1: Agency Practices and Supported Outcomes

Practice										
	1. Programs and projects frequently deliver valuable product									
	2. Value is continuously discovered and aligned to mission									
	3. Work flows in small batches and is validated									
	4. Quality is built in									
	5. The organization continuously learns and improves									
	6. Teams collaborate across groups and roles to improve flow and remove delays									
	7. Security and compliance constraints are embedded and verifiable									
	8. Consistent and repeatable processes across build, test, and deploy									
	9. The entire system is deployable at any time to any environment									
10. The system has high reliability, availability, and serviceability										
Delivery Cadence	X		X				X	X		
Delivery Environment	X		X			X	X	X		
Iterative, Incremental Development	X	X	X		X		X	X		
Embedded Product Ownership	X	X			X	X	X			
Representation of Requirements	X	X	X			X		X		
Automated Testing	X		X	X			X	X	X	X
Fail-Safe	X		X	X			X	X	X	X

Practice	Extrinsic Quality	X	X	X							1. Programs and projects frequently deliver valuable product
	Intrinsic Quality	X		X	X						2. Value is continuously discovered and aligned to mission
	Emergent Design	X									3. Work flows in small batches and is validated
	Refactoring	X		X	X						4. Quality is built in
	Intentional Architecture		X		X						5. The organization continuously learns and improves
	Managing Technical Debt	X		X	X						6. Teams collaborate across groups and roles to improve flow and remove delays
	Version Control			X		X					7. Security and compliance constraints are embedded and verifiable
	Scripted Builds						X	X			8. Consistent and repeatable processes across build, test, and deploy
									X		9. The entire system is deployable at any time to any environment
					X	X				X	10. The system has high reliability, availability, and serviceability

Practice		1. Programs and projects frequently deliver valuable product							
		2. Value is continuously discovered and aligned to mission							
Automated Builds		3. Work flows in small batches and is validated	X						
Scripted Deployment		4. Quality is built in	X						
Deployment with minimal downtime for users	X	5. The organization continuously learns and improves							
Automated Deployment	X	6. Teams collaborate across groups and roles to improve flow and remove delays				X			
Approved Pipeline	X	7. Security and compliance constraints are embedded and verifiable							
System Monitoring		8. Consistent and repeatable processes across build, test, and deploy					X		
Release Planning		9. The entire system is deployable at any time to any environment	X						
Visibility of progress	X	10. The system has high reliability, availability, and serviceability	X						

Practice Peer reviews Integrated Experimentation & Learning Culture of learning Deployment History and Consistency				1. Programs and projects frequently deliver valuable product
				2. Value is continuously discovered and aligned to mission
				3. Work flows in small batches and is validated
				4. Quality is built in
				5. The organization continuously learns and improves
				6. Teams collaborate across groups and roles to improve flow and remove delays
				7. Security and compliance constraints are embedded and verifiable
				8. Consistent and repeatable processes across build, test, and deploy
				9. The entire system is deployable at any time to any environment
				10. The system has high reliability, availability, and serviceability



**U.S. Citizenship
and Immigration
Services**

USCIS

Management Instruction for Agile Independent Verification and Validation (IV&V)

Management Instruction: CIS-OIT-004

June 2017

Unclassified

Version 1.0

ITDL Number: 211137

This document was prepared for authorized distribution only.

This page left intentionally blank.

Office of Information Technology

Management Instruction for Agile Independent Verification and Validation

Effective Date: 26 June 2017

Management Instruction: CIS-OIT-004

I. Purpose

This Management Instruction (MI) establishes the U.S. Citizenship and Immigration Services (USCIS) policy for the use of risk-based Independent Verification and Validation (IV&V) to inform management and make oversight decisions ensuring that Information Technology (IT) programs adhere to USCIS Management Instruction CIS-OIT-003 and its Appendices.

The primary functions of USCIS IV&V are:

- Provide transparency and accountability to the public;
- Provide timely feedback to program executors to continuously improve processes, practices, and outcomes;
- Ensure that projects deliver solutions that meet business objectives, support mission needs, and deliver value;
- Inform management and oversight bodies with an independent assessment of program execution based on data and analysis;
- Ensure compliance with regulatory requirements, USCIS Management Instructions, and Department of Homeland Security (DHS) Management Directives

To fulfill these functions, USCIS IT programs will use a risk-based IV&V approach to verify and validate the outcomes defined in Management Instruction CIS-OIT-003 and its Appendices. The IV&V process will ensure that the appropriate controls and analyses are applied to each program based on its assessed risk. The approach for each program will be agreed upon through a collaboration of program executors, USCIS management, IV&V teams, and external stakeholders, and will be documented in a new document called the Independent Assessment Plan (IAP).

II. Scope

This Management Instruction focuses on the IV&V program at USCIS but applies to all employee and contractor teams involved in the planning, development, and deployment of software and systems throughout USCIS.

III. Authorities

The following laws, regulations, orders, policies, directives, and guidance authorize and govern this Management Instruction:

1. DHS Management Directive (MD) 102-01 "Acquisition Management Directive," and associated Instructions and Guidebooks
2. Section 5202 of the Clinger-Cohen Act of 1996
3. Office of Management and Budget (OMB) Circulars A-130 and A-11
4. 25 Point Implementation Plan to Reform Federal Information Technology Management (U.S. Chief Information Officer, December 9, 2010)
5. Contracting Guidance to Support Modular Development (OMB, June 14, 2012)
6. Memorandum on Agile Development Framework for DHS, by DHS CIO Richard A. Spires, issued June 1, 2012
7. Digital Services Playbook (<https://playbook.cio.gov>)

IV. Policy, Procedures, and Requirements

Except in cases where a waiver is granted by the Chief Information Officer (CIO), all systems development and maintenance projects at USCIS will require IV&V. Such projects include, for example, custom software development, Commercial Off-The-Shelf (COTS) integration and configuration, business intelligence, and reporting capabilities.

USCIS Office of Information Technology (OIT) management will ensure that appropriate training, coaching, and tools are available to facilitate the success of all projects. Teams are encouraged to work with OIT support groups to implement this Management Instruction in a manner appropriate for their particular context.

A. IV&V Approach

The IV&V approach to each release cycle of each project is based on a holistic assessment of the project, the team's development history, the release plan, and the deployment plan. This assessment is based on the unique characteristics and measures of each assessed element. Some examples include:

- DHS program level or CIO designation for the project
- Visibility to the public
- Impact on mission critical systems
- Number of internal and external users affected
- Federal Information Processing Standard (FIPS) rating and security or privacy impacts
- Reliance on interfaces to external systems
- Development process
- Outcomes to date (e.g., technical debt, escaped defects, user satisfaction)

At the beginning of each project, the IV&V stakeholders will evaluate the project's risk and create an Independent Assessment Plan (IAP). The IAP will be re-evaluated from time to time during the course of the project to see if it needs to be changed. The IAP will indicate what level of assessment will be conducted, what resources will be allocated, and what templates will be used for assessment. Appendix C to this document shows an example of an IAP template (the template may vary over time). The IAP will serve as a guide for IV&V as the program proceeds.

USCIS has also developed an assessment tool called the Product Quality Assessment (PQA) that will be continuously refined as USCIS OIT gains experience determining the success factors for projects. An example is shown in Appendix B of this document. This instrument will be the default template for IV&V assessments of major programs. The PQA compares the program's practices and status to the instructions given in Management Instruction CIS-OIT-003 and in its Appendix A. The IV&V process therefore functions as a control to ensure that programs implement the direction specified in Management Instruction CIS-OIT-003 and its Appendices.

There will be a direct correlation between risk and the level of IV&V engagement. High risk programs (all level one and two programs and certain level three programs) will have embedded IV&V analysts and testers working with the development team, while low risk programs may only be audited. High risk programs will also be assessed more frequently than low risk programs. IV&V will also evaluate and provide feedback on all Systems Engineering Lifecycle (SELC), Acquisition Lifecycle Framework (ALF), and other oversight documents and artifacts.

Key documents, artifacts, and relevant risk assessments will be revisited in each Release Planning Review (RPR) and will be updated as necessary, depending on the level of IV&V engagement, throughout the release cycle.

During project execution, IV&V teams will monitor team progress toward the outcomes set forth in USCIS Management Instruction CIS-OIT-003 and its Appendices. Depending on the needs of the project, IV&V teams may also include other activities such as:

- Sample testing for Section 508 conformance
- Code quality scanning and manual code review
- Unit test review
- Functional testing and test review
- Integration testing
- Performance testing
- End User testing

These activities will inform IV&V teams' analysis as documented in the PQA. IV&V will execute these activities in a manner that supports agile delivery practices and methods.

B. Team Managed Deployment

In order to support best practices for DevOps and Continuous Delivery techniques, USCIS has developed a methodology called, *Team Managed Deployments* (TMD). In order to engage in this methodology, a program must be onboarded to TMD by the IV&V stakeholders. In assessing eligibility for TMD, IV&V stakeholders will evaluate a program's readiness relative to CIS-OIT-003 Outcomes #7, #8, #9, and #10. The results of the evaluation and a determination for TMD certification will be conducted as part of the program's next RPR, in accordance with Management Instruction CIS-OIT-003. Example measurements are provided in Appendix A.

C. Value Delivery

A primary function of IV&V at USCIS is to ensure projects deliver solutions that meet business objectives, support mission needs, and deliver value. This work begins in release planning, when the IV&V team works with Product Owners to ensure that teams plan to deliver capabilities that clearly meet mission needs and priorities, as outlined in the Capabilities and Constraints (CAC) document.

At RPR, IV&V ensures alignment with business needs by validating that the appropriate stakeholders (product owners, line of business executives, etc.) are present in person or by delegation and fully approve release plans. During the development cycle, IV&V monitors projects to ensure that business representatives are involved in work planning sessions, and in monitoring and participating in test efforts.

For Level 1 and other designated projects, IV&V also supports Operational Test & Evaluation (OT&E). OT&E, or Operational Testing, is a testing process that takes place on production systems with production data with real end users. Its purpose is to determine whether Key Performance Parameters (KPPs) articulated in the Measures of Effectiveness (MOEs) and Measures of Suitability (MOSs) set forth in the Operational Requirements Document (ORD) by the business sponsor at program authorization have been met, or not. Many experts consider this the ultimate test of business value, as it was what was promised when the program was authorized.

V. Questions, Comments, and Suggestions

Please address any questions, comments, or suggestions to: USCIS-QA-TEAM@uscis.dhs.gov

VI. Approval

Signed:  Date: 06/26/2017

Appendix A: Example Metrics

Below are examples of measurements supporting evaluation of objective outcomes. Key measurements must be agreed among program management, IV&V, and USCIS OCIO for regular reporting. The agreement on measurements must be recorded in the POP, and revisited in each RPR. This list is neither mandatory nor exhaustive, but serves as an indicator of the types of measurements that should be considered in crafting the POP for a specific program.

MI CIS-OIT-003 Outcome	Examples of IV&V Decision Support Measurements (Trending Preferred)
Outcome #1: Programs and projects frequently deliver valuable product	<ul style="list-style-type: none"> • Quantitative measurements of program goals (business KPIs) • Number of deployments • User satisfaction • Strategic stakeholder satisfaction • Usage statistics
Outcome #2: Value is continuously discovered and aligned to mission	<ul style="list-style-type: none"> • Lead times for new functionality • Evidence of feedback being incorporated
Outcome #3: Work flows in small batches and is validated	<ul style="list-style-type: none"> • Work item flow measurements (e.g. cycle time) • Batch size • Evidence of test coordination • Evidence product demonstration feedback is incorporated in requirements
Outcome #4: Quality is built in	<ul style="list-style-type: none"> • Incident count (escaped defects) • Code quality measurements • Test coverage • Evidence of appropriate tool configuration and use
Outcome #5: The organization continuously learns and improves	<ul style="list-style-type: none"> • Amount of effort spent on improvement • Outcomes of retrospective experiments • Implementation of retrospective action items • Evidence of appropriate measurement activities • Evidence of feedback being incorporated • Evidence of practice transfer across organization

MI CIS-OIT-003 Outcome	Examples of IV&V Decision Support Measurements (Trending Preferred)
Outcome #6: Teams collaborate across groups and roles to improve flow and remove delays	<ul style="list-style-type: none"> • Continuous integration availability • Lean measurements • "Health check" assessment of team practices
Outcome #7: Security, accessibility and other compliance constraints are embedded and verifiable	<ul style="list-style-type: none"> • Cost of compliance issues to customers, users, and agency • Number of open issues • Security risk level • Section 508 risk level • Privacy risk level • Performance risk level
Outcome #8: Consistent and repeatable processes are used across build, deploy, and test	<ul style="list-style-type: none"> • Rate of broken builds, particularly in later stage gates • Number/percentage of escaped defects
Outcome #9: The entire system is deployable at any time to any environment	<ul style="list-style-type: none"> • Percentage of deployments needing rollback • Pipeline and repository unavailability incidents
Outcome #10: The system has high reliability, availability, and serviceability	<ul style="list-style-type: none"> • Incident count • Incident aging and inventory • Escaped defect count • Uptime • Production performance • Mean time to repair • Mean time between failures • Production error count

Appendix B: Product Quality Assessment (PQA) Tool

Assessment Summary: DID (It) - RTT - Release # 3.0				Step 1: Complete	Step 2: Complete	Step 3: Complete	
PORTFOLIO	SYSTEM	RELEASE #	MISSION CRITICAL	REL. START DATE	REL. END DATE	CONTRACT END DATE	SELECT DEPLOYMENT
DID (It) RoR	DID (It) - Ride The Tide	3.0	Not Mission Critical	Rel. Start Dt: 03/05/2017	End Dt: 09/04/2017	12/31/2020	3.6
Team	QUALITY ENGINEER		QUALITY ENGINEER	SECTION 508 IV&V	SECTION 508 IV&V	KEY STAKEHOLDER(S)	VENDOR
	McElroy, Kerry B		White, Giezelle M	Kouznetscva-Smith, Olga M	Malik, Ahsan J	John Smith, Sally Smith, Bill Smith	CompuGenex
System Info	SECTION 508 EXEMPTION		SECTION 508 EXPOSURE	CR REQUIRED	FIPS	ECN SITE	CONTRACT
	Not Exempt. MUST be Section 508 Compliant		Internal applications supporting 251-2,530 people	The system does NOT require a CR or ICCB approval to deploy to production	LLL	http://ecn.uscis.dhs.gov/team/esd/Division/Verification/VERMOD/VISDEV/VIS%20Wiki/Release%20Planning%20Review.aspx	Eagle - II
Recommendations Summary	QA FINDINGS & RECOMMENDATIONS SUMMARY						
	GITHUB	PIV	SECTION 508 RISK LEVEL	ATO STATUS	DEPLOYMENT FREQUENCY	BROWSER NEUTRALITY	
	All Code and Deployments from GitHub	100% PIV Enabled	High System Maintains High Section 508 Compliance	System has its own Valid ATO with more than more than 6 months to expire	System Part of a Portfolio - NO Has Had a Deployment in the Past 90 Days - Yes	System has been Tested & Works with Latest Version of Chrome, IE	
	TMD STATUS	MOU PERFORMANCE	DEPLOYMENT RISK LEVEL	DEPLOYMENT RISK SCORE	RPR READINESS	RRR READINESS	
	System was Recently Assessed for TMD, Approved PDD, but not TMD Approved yet	No History of MOU QE Does NOT Recommend MOU for This Release	LOW Risk (Q4) Assess 1st, 4th....& Final Deployment	Consequence: 18515 Likelihood: 21115	N/A b) DAB Conditional Concurrence - Action Items Identified	Team NOT READY, UNRESOLVED Risks/Issues (An Interim Deployment) b) DAB Conditional Concurrence - Action Items Identified	
	PROCUREMENT	PLANNING	DESIGN & BUILD	TESTING	IMPLEMENTATION	OPERATIONS	OTHER
	ISSUES	0	4	0	0	0	0
	RISKS	0	13	4	1	13	3
	Total ISSUES IDENTIFIED	CRITICAL	HIGH	MEDIUM	LOW	Total UNRESOLVED	
	4	0	0	1	2	4	

Appendix C: Independent Assessment Plan (Example¹)

Independent Assessment Plan for *ABC Project*

Basis

This plan is based on a consolidated risk assessment of the program, application, development team, and release planning documents by IV&V stakeholders from the Applied Technology Division (ATD) and Information Security Division (ISD), working in concert with oversight bodies from the Department of Homeland Security (DHS). It was developed in consultation with the project team over a series of discussions that took place from May 1-7. The risk assessment working document is the Product Quality Assessment (PQA) artifact for this release, filed under ITDL number 1234567.

Assessed Risk Level: Medium

This is an enterprise application with a strong project team, no outstanding security POAMs or Section 508 defects, and a limited number of system interfaces. The FISMA rating for this system is MMM and it supports PII data. Capabilities planned for this release do not appear to be especially challenging or risky. Normally, this would call for a lower risk rating. During the course of this release, however, two of the four development teams are transitioning to a new Contractor. In addition, the program is working on a requirement from external auditors to improve customer satisfaction ratings.

Feedback Loops

Activity (what)	Used (Yes/No)	Frequency (when – specific tempo or dates)	Explanation (why)
Release Planning Review (RPR)	Yes	Once – authorizes release start	Required for all releases unless waived in writing by the CIO; this RPR was not waived.
Independent Assessment Reports (IAR)	Yes	One per month	Contract teams are due to turn over on June 16th so these two reports will provide a good before and after view of the program.

¹ This is a sample version of the IAP template at the time of publication for MI 004. This template will evolve and change as we inspect, adapt, and iterate.

Independent Assessment Plan for ABC Project

Activity (what)	Used (Yes/No)	Frequency (when – specific tempo or dates)	Explanation (why)
Release Status Review (RSR)	Yes	<i>For this release, RSR will take place once, before new teams engage in development activities.</i>	<i>To confirm that all RPR agreements are still valid.</i>
Release Readiness Review (RRR)	Yes	<i>For each deployment</i>	<i>This project is not yet authorized for TMD or MOU processing, so a review will be required for all deployments. The deployment for Capability #3 and the first two deployments involving the new teams will be full RRR meetings; all others will be eRRRs.</i>
Post Implementation Review (PIR)	Yes	<i>At the end of the Release (no later than 11/17/2017)</i>	<i>No waiver has been issued so this review is required.</i>

Quality Assurance Activities

Activity (what)	Used (Yes/No)	Frequency (when – specific tempo or dates)	Explanation (why)
Planning support / assessment	Yes	<i>Once per month</i>	<i>This is a high cadence for a medium risk project but we want to compare before and after team transition to catch problems early.</i>
Demo support / assessment	Yes	<i>Once per month</i>	<i>See note above.</i>
Backlog support / assessment	Yes	<i>At RPR, RSR, and PIR</i>	<i>See note above.</i>
Retrospective	Yes	<i>At RPR and at least three times after RSR</i>	<i>See note above.</i>

Independent Assessment Plan for *ABC Project*

Activity (what)	Used (Yes/No)	Frequency (when – specific tempo or dates)	Explanation (why)
Kanban support / assessment	Yes	At random sometime after RSR	See note above.
Pipeline audit	No		See note above.
Independent code review	No		Program is conducting peer review and there are no known problems that justify independent assessment.
Metrics review	Yes	Prior to PIR	This is standard. Program has selected the follow key measurements: Deployment frequency; WIP; cycle time.
Design review	Yes	Prior to PIR	This is standard and will be scheduled sometime after Iteration 4.
ITDL audit	Yes	Prior to RSR and PIR	We must ensure that documents have been filed properly before team transition and prior to PIR.
Release Self Governance MOU	No		Not requested.
TMD Readiness Assessment	No		Not requested at RPR and not anticipated for this release.
Other			

Independent Assessment Plan for ABC Project

Independent Testing Activities

Activity (what)	Used (Yes/No)	Engagement Level (Method and frequency of engagement)
Enterprise Test Readiness	Yes	<i>For each Release from Production</i>
Post-Implementation Test Readiness Review	No	<i>After each Deployment Release</i>
Testing Retrospective	No	<i>After each Deployment Release</i>
Test Management: Monitoring	No	<i>After each Release from Production and after each Deployment Release</i>

Other Support Activities

Activity (what)	Used (Yes/No)	Engagement Level (Method and frequency of engagement)
Training	Yes	<i>DAB has agreed to coordinate an on-boarding session for the new contractor teams.</i>
Coaching	Yes	<i>ACT has agreed to provide a coach for the new contractor teams.</i>
Pipeline Engineering	No	
Value Team Partnership	Yes	<i>DAB has agreed to support product discovery meetings and activities; participate in user research and usability testing; and assist in developing hypotheses and running experiments (fostering the build - measure – learn loop).</i>
Daily Stand Up	Yes	<i>ACT has agreed to support daily standup meetings on request for the first two iterations and DAB will attend them at random to monitor release activity.</i>

Appendix D: Independent Assessment Report (Example²)

Independent Assessment for [Portfolio/Program/System]

[Report Period]

Report Goals

- Identify changes (including all outages and deployments) that materially impact the program mission
- Assess the quality of the program against outcomes required by USCIS Management Instructions for Lean, Agile and DevOps (MI CIS-OIT-003)
- Provide key facts and measurements that assist USCIS management in transparency, public accountability, effective oversight, and efficient execution of the Program

Ops Data Sources

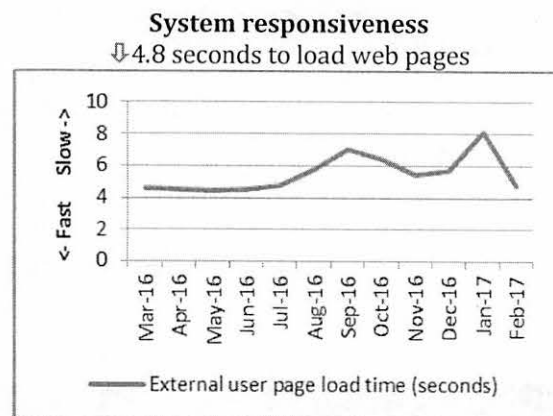
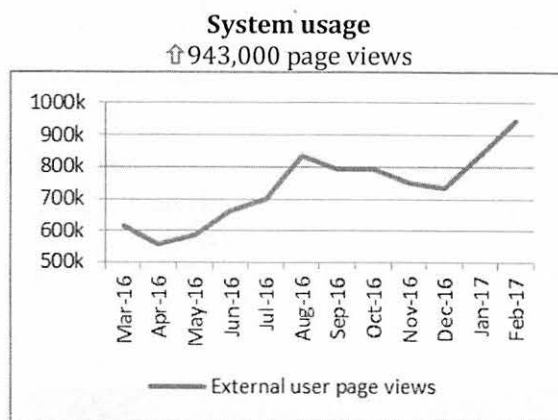
[Links to data sources]

Production Report (Ops to Dev Feedback)

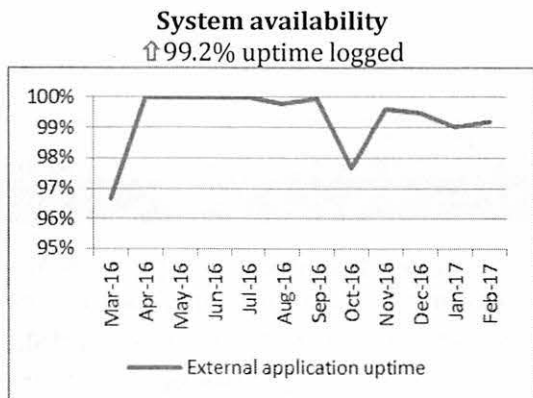
USCIS IV&V recognizes that amplifying and acting on production feedback is a foundational technique used to align program activities with the immediate needs of USCIS customers, business stakeholders, and system operators.

Customer Experience

[Instructions: Provide system operations measurement – examples provided]



² This is a representation of the IAR template created at a point in time for one active Program. The actual content for each IAR may be similar but will vary based on the needs of the underlying program at that time. The template itself will also change as we inspect, adapt, and iterate.



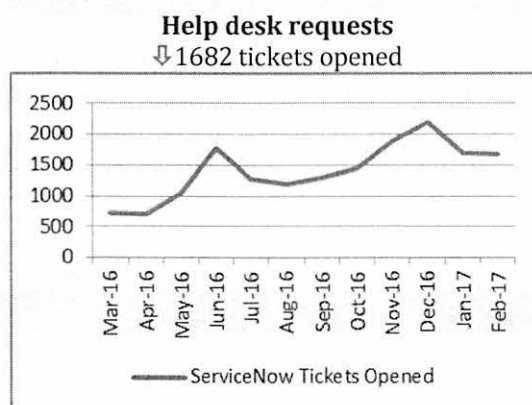
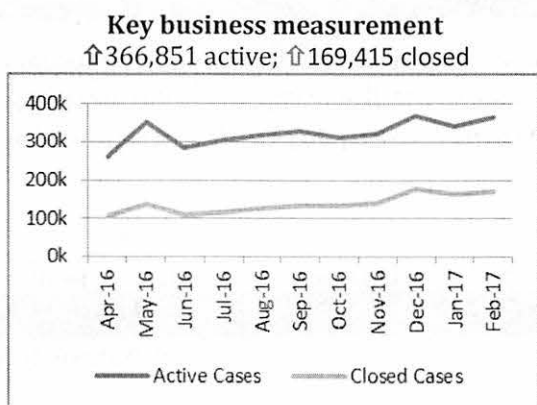
Outage Events

↓ 3 outages -- ↑ 5h29m downtime

	Duration	Highlights	Planned
2/2	20 min	Load spike	No
2/10	9 min	Virtual server autoscaling problem	No
2/28	~5 hours	Major cloud component outage	No

Business Measurements and User Feedback

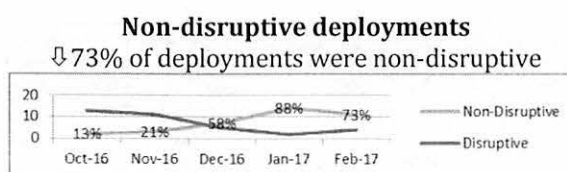
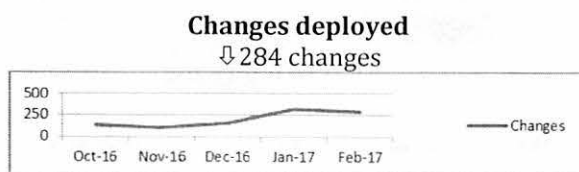
[Instructions: Provide measurements of key business objectives for the system – examples provided]

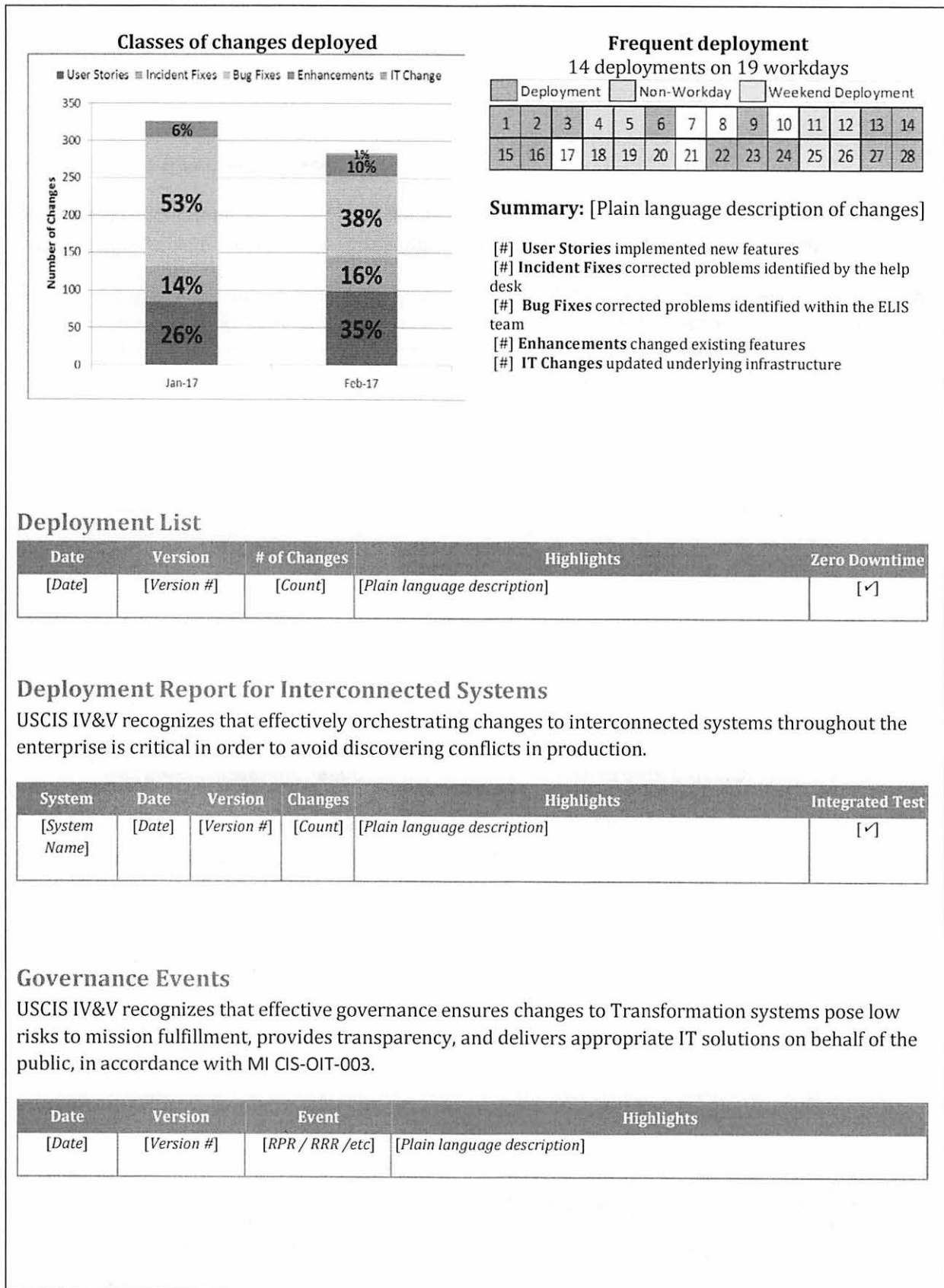


Deployment Report (Workflow from Dev to Ops)

USCIS IV&V recognizes that frequently deploying software is a foundational technique used by the XYZ Program to deliver quality product and prevent work flowing backwards. In addition, frequent deployments continuously improve program capability to reliably build, test, and deploy software following MI CIS-OIT-003.

[Instructions: Provide measurements related to deploying changes to production, including information about deployments, classes of changes, testing, and code quality – examples provided]





Attachment 8 - Management Instruction for Agile Independent Verification and Validation (IV&V)

Report on Changes to Program Outcomes

USCIS IV&V recognizes that DevOps practitioners must work within a culture of continuous improvement. This section describes material changes to Transformation Program outcomes, in order to provide a picture of the program's overall capacity for continuous improvement. Outcomes are listed in accordance with MI CIS-OIT-003. The color-coding indicates the IV&V team's judgment on whether the change is trending positive or negative.

Trending Positive (Green)	Trending Negative (Yellow)	Significant Negative Impact (Red)
--------------------------------------	---------------------------------------	--

Outcome	Description	Last Reported	This Month's Topics	Future Topics
1	Programs and projects frequently deliver valuable product	This Month	Trending Positive	
2	Value is continuously discovered and aligned to mission	This Month	Trending Negative	
3	Work flows in small batches and is validated	This Month	Trending Negative	
4	Quality is built in	This Month	Trending Negative	
5	The organization continuously learns and improves	Jan 2017	Not reviewed	
6	Teams collaborate across groups and roles to improve flow and remove delays	This Month	Trending Positive	
7	Security and compliance constraints are embedded and verifiable	Jan 2017	Significant Negative Impact	
8	Consistent and repeatable processes are used across build, test, and deploy	Jan 2017	Not reviewed	
9	The entire system is deployable at any time to any environment	N/A	Not reviewed	
10	The system has high reliability, availability, and serviceability	This Month	Trending Positive	

[Describe IV&V selected outcome, assessment question, evidence, analysis, and recommendations]

Outcome 1: Programs and projects frequently deliver valuable product

[Plain language title
describing material change
to outcome]

**Sustained increase in
deployment frequency**

[Trending Direction]

Trending Positive

[Recommendations]

Recommendation: Aim for one deployment every workday

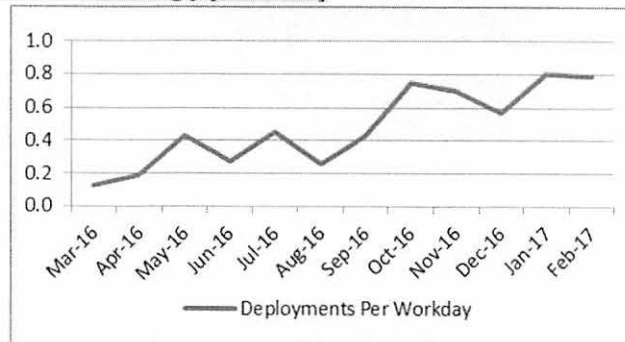
[Assessment question from CIS-OIT-003]

Assessment Question: How frequently is the working functionality delivered to end users for use?

[Description of assessment method]

To answer this question, the IV&V team counted the number of deployments in the last 12 months.

[Evidence – data strongly preferred]



[IV&V analysis narrative]

We observed a sustained increase in the number of deployments since October 2016. As a result, the program demonstrated a reliable capability to build, test, and deploy the application. Major factors likely include:

- Introducing zero downtime deployments (ZDD)
- Adopting a daily deployment cycle with prompt testing for each release candidate
- Ownership of the deployment process by rotating Release Captains

1. **Escaped Defects:** An escaped defect is a code error that was not discovered by DevOps teams during development and testing prior to deployment to production. Typically, escaped defects are discovered by end users shortly after a production deployment, at which time, the impact on business operations and user experience is high. There are a number of potential underlying causes, such as erroneous or missing code, misconfiguration, logic and architecture issues, data quality errors, and timing/serialization conflicts, to name a few. The Government's expectation is any defect with significant business impact should be resolved immediately, to include understanding and addressing the root cause of the problem. Understanding that factors such as defect severity and complexity will drive the time needed for root cause analysis and resolution, the Government's priority is to first return production to normal/steady-state operations, followed by root cause analysis and resolution.
2. **Alpha and Beta Testing:** The Transformation program has incorporated user-facing testing practices throughout its continuous delivery lifecycle in order to improve product quality, adoption, and user satisfaction. The program conducts Alpha/Beta (A/B) testing with users to collect evidence-based feedback on critical defects, user experience issues, misalignment of features to business requirements, as well as interoperability problems. Transformation A/B testing has proven to be an accurate, incremental, and time-effective means of obtaining feedback prior to the nationwide roll-out of new or enhanced product lines and capabilities.
3. **Deployable verses deployed:** DevOps team responsibilities do not end with development; teams are responsible for deployments and production support as well. The program practices continuous delivery (CD), where code changes are automatically built, tested, and prepared for deployment to pre-production and production environments after the build stage. The goal here is to keep the codebase in a deployable state at any given time.
4. **DevOps verses DevSecOps:** DevOps represents cultural philosophies, practices, and tools that are all combined to quickly deliver digital products and services with maximum business value. DevOps engineers work across the entire delivery lifecycle (from development, testing, deployment, and operations), and possess a range of skills traditionally handled by separate teams such as quality assurance, infrastructure, and security.
5. **Microservices Architecture:** The program's microservices architecture is a design approach to building an application as a set of small services. Each microservice is built around business capabilities that are prioritized by the Government. Each service is scoped to a single purpose, runs in its own process, and communicates with other services through a well-defined application programming interface (API). Each microservice is built on an OpenShift platform so it runs in its own pipeline and can be deployed independently, as a single service, or as a group of services.