DEPARTMENT OF HOMELAND SECURITY (DHS)
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)
HOMELAND SECURITY INVESTIGATIONS (HSI)
OFFICE OF INTELLIGENCE (INTEL)
STATEMENT OF WORK (SOW)
FOR
ShadowDragon SocialNet through Maltego

1.0 GENERAL

Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Office of Intelligence (INTEL) has a broad and complex public safety mission which is furthered through the collection and sharing of timely and accurate intelligence on illicit trade, travel, and financial activity with a nexus to the United States.

1.1 BACKGROUND

HSI INTEL has a responsibility for identifying and exploiting emerging data from traditional and non-traditional sources which can significantly enhance its's capability of furthering ICE's mission. ICE analysts conduct research on readily available public domain open source information that spans beyond US domain websites and require ICE to effectively track and investigate known criminal elements and locations to mitigate the flow of illegal goods and personnel into the United States borders and territories. SocialNet data is a data subscriptions service that maps social media connections to uncover aliases, associates and gather inferences of lifestyle and physical location of threats. SocialNet performs federated searches and visualizes social media connections to uncover identities, correlations, networks of associates quickly.

HSI INTEL must remain diligent in seeking new and improved means of combatting the challenges that face our Law Enforcers and Intelligence Analysts for identifying, tracking, investigating and apprehending criminal entities. SocialNet data adds to HSI INTEL's ability to successfully meet those mission goals and their public responsibility by leveraging capabilities with proven results for both cyber or physical criminal investigations and social media forensics.

1.2 SCOPE

The purpose of this requirement is to provide HSI INTEL with one (1) base year SocialNet access through the Maltego platform application with 100 licenses at or greater than 250 daily queries per licenses.

1.3 OBJECTIVE

HSI INTEL is seeking to procure ShadowDragon (manufacture) SocialNet on a Brand Name sole source basis. Due to rapidly advancing technology and the need to remain vigilant, HSI INTEL must continuously identify tools that can enhance and support ICE's law enforcement and intelligence mission. ShadowDragon SocialNet access is provided through the Maltego

application. The platform can be installed on *non-IRMNET* laptops currently deployed across the HSI enterprise.

ShadowDragon develops cyber intelligence solutions that provide threat-related information to organizations, enabling them to stop and attribute targeted actions of malicious actors in the physical or digital world. These solutions are achieved through monitoring and analyzing data from proprietary threat databases, the Internet and the dark web.

SocialNet is a unique interactive data mining tool that renders directed graphs for link analysis. The results are visualized in minutes to reveal detailed 1 to 1 correlation as well as larger networks of associates. Features include:

- Easy, fast, and reliable visualization of people's profile information and relationships
- Search 60+ social networking sites and other account based online entities.
- Complete multiple queries in minutes, which would take hours or days to complete manually.
- Visualize 1 to 1 correlations as well as multiple relationships and networks of people into the 1000s of records.
- Reliable and accurate results with a proprietary data collection/query methodology that has been refined over five years and is continually updated.

HSI INTEL analysts conduct research on readily available public domain open source information spanning beyond US domain and the nature of ICE investigations spans across national borders and languages. The need for tools that capture social networking digital tracks with abilities to pull and extract relevant/useable intelligence information are vital for HSI-INTEL to accomplish its mission and support their basic requirements.

The Government requirements are:

The Government requires a database with the capacity to analyze large amounts of multi-lingual data from disparate sources in near real time by leveraging publicly available information through a geo-enabled, text analytics, social media, and web-monitoring platform.

The Government requires a database with the ability to glean information from multiple sources, including, but not limited to:

(b)(7)(E)

DEPARTMENT OF HOMELAND SECURITY (DHS)
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)
HOMELAND SECURITY INVESTIGATIONS (HSI)
OFFICE OF INTELLIGENCE (INTEL)
STATEMENT OF WORK (SOW)
FOR
ShadowDragon SocialNet through Maltego

(b)(7)(E)

The Government requires a database to maintain continuous access to major social media sites.

The Government requires that the database platforms must have the capability to:

(b)(7)(E)

The Government requires a database to filter results on a wide range of variables determined by the user; such as keywords, hashtags, language, author, emoji, dates, times, expression.

The Government requires a database to create user defined analysis based upon network connections, sentiment, significance, reach, popularity, key influencers, concepts, named entities, trends, data type and filters. The database platform must be able to analyze and map network connections, obtain content of investigative interest, and assist users in determining threat postings warranting protective actions.

The Government requires a database that can accurately and near real time execute the following searches with multi-lingual capability:

(b)(7)(E)

1.4 APPLICABLE DOCUMENTS

Official Proposal Not Received, to date.

2.0 PERIOD OF PERFORMANCE

DEPARTMENT OF HOMELAND SECURITY (DHS)
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)
HOMELAND SECURITY INVESTIGATIONS (HSI)
OFFICE OF INTELLIGENCE (INTEL)
STATEMENT OF WORK (SOW)
FOR
ShadowDragon SocialNet through Maltego

The proposed period of performance is one (1) base year.

2.1 PLACE OF PERFORMANCE

Immigration and Customs Enforcement, Homeland Security Investigations

2.2 INTELLECTUAL PROPERTY

Office of Principal Legal Advisor (OPLA), Commercial and Administrative Law Division (CALD) will review this requirement for Intellectual property applicability as needed.

2.3 SECTION 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

4.0 GOVERNMENT FURNISHED RESOURCES

The Government will not furnish any resources to the Contractor in support of this contract.

5.0

MARKET RESEARCH MEMORANDUM

TO: Contracting Officer/Specialist *(I.E. CONTRACTING OFFICER/SPECIALIST)*

FROM: HSI Intelligence, IESD (b)(6); (b)(7)(C)

SUBJECT:

ShadowDragon Maltigo Licenses

DATE: 4/27/2020

This memorandum is in accordance with Federal Acquisition Regulation (FAR) Part 10.000, which describes the policies and procedures for conducting market research to reach the most suitable approach to acquiring, distributing, and supporting supplies and services. This Part implements requirements of 41 U.S.C. 253a (a) (1), 41 U.S.C. 264b, and 10 U.S.C. 2377.

I. BACKGROUND

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), the largest investigative agency in the U.S. Department of Homeland Security (DHS), protects national security by enforcing the nation's immigration and customs laws. ICE HSI Office of Intelligence (Intel) has a broad and complex public safety mission which is furthered through the collection and sharing of timely and accurate intelligence on illicit trade, travel, and financial activity with a nexus to the United States. Intel leads this agency-wide continuity of operations, emergency response and crisis management to include establishing and maintaining an agency-wide secure data communication connectivity. One of the leading priorities of HSI Intel is to combat criminal activity conducted on or facilitated by the Internet. HSI Intel delivers computer-based technical services to HSI components to support domestic and international investigations into cross-border crimes. HSI Intel is comprised of the Intelligence Analysis Division, Intelligence Collection Division, Intelligence Integration & Emergency Management Division and Intelligence Enterprise Services Division.

II. REQUIREMENT

HSI-INTEL has a requirement on a Brand Name sole source basis to purchase ShadowDragon

cyber investigation SocialNet through the Maltego platform tool for on (1) base year. Due to rapidly advancing technology and the need to remain vigilant, HSI-INTEL must continuously identify tools that can enhance and support ICE's law enforcement and intelligence mission.

ShadowDragon SocialNet access is provided through the Maltego application. The platform can be installed on NON-IRMNET laptops currently deployed across the HSI enterprise. This requirement is to allow HSI-Intel access to ShadowDragon SocialNet.

ShadowDragon develops cyber intelligence solutions that provide threat-related information to organizations, enabling them to stop and attribute targeted actions of malicious actors in the physical or digital world. These solutions are achieved through monitoring and analyzing data from proprietary threat databases, the Internet and the dark web. ShadowDragon is used to by hundreds of private businesses, intelligence and law enforcement organizations globally.

ShadowDragon, will allow HSI-INTEL access to the tools, identified below, in support of its investigative mission(s):

SocialNet is a unique interactive data mining tool that renders directed graphs for link analysis. The results are visualized in minutes to reveal detailed 1 to 1 correlation as well as larger networks of associates. Features include:

- Easy, fast, and reliable visualization of people's profile information and relationships
- Search 60+ social networking sites and other account based online entities.
- Complete multiple queries in minutes, which would take hours or days to complete manually.
- Visualize 1 to 1 correlations as well as multiple relationships and networks of people into the 1000s of records.
- Reliable and accurate results with a proprietary data collection/query methodology that has been refined over five years and is continually updated.

III. DELIVERY/PERFORMANCE TIME

Need by date: 9/1/2020
Base Period of Performance (POP) dates: *From* 9/7/2020 *To* 9/6/2021

Click the link to see if the need is "Urgent":
http://intranet.ice.dhs.gov/sites/oaq/resources/palt.htm

☒No
☐Yes (Urgent Justification Form Required)

IV. METHODOLOGY OF MARKET RESEARCH

The results of market research have determined that the Government's needs can be met by:

☐Items of a type customarily available in the commercial marketplace;
☐Items of a type customarily available in the commercial marketplace with modifications; or
☒Items used exclusively for governmental purposes.

The following methods were utilized to conduct Market Research:

☐FedBizOpps Sources Sought Synopsis (https://www.fbo.gov/)
☒GSA/FSS (GSA Advantage)
https://www.gsaadvantage.gov/advantage/main/start_page.do)
☐Unicor (http://www.unicor.gov/)
☐JWOD/AbilityOne (http://www.abilityone.gov/)
☒SAM (https://www.sam.gov/portal/public/SAM/)
☐Previous purchases of similar/identical items
☐Internet
☐Contacted SBA (http://www.sba.gov/)
☒Firstsource II (http://mgmt-opo-sp.dhs.gov/sites/epic/Pages/FirstSource%20II.aspx)
☒Other (***Please Explain)***: Single Source
☒Other Strategic Source (BPA, IDIQ, etc.)

Ex: http://dhsconnect.dhs.gov/org/comp/mgmt/cpo/oss/Pages/StrategicSourcing.aspx)

Ex: TacCom Motorola HSSS01-12-D-0002)

V. SUMMARY OF MARKET RESEARCH

HSI Intel conducted market research through internet, Strategic Source and GSA Advantage. In total three (3) cost estimate was received. This shows that competitive pricing can be found and recommends this requirement be re-solicited to each of the vendors to provide a more competitive purchase.

The apparent fair market value based on the Market Research conducted ranges between $(b)(4) and $(b)(4) for 100 licenses annually with a minimum of 250 daily query limit per license.

Vendor Name	Vendor POC	Vendor Info	Estimated Cost	Comments
Shadow Dragon	(b)(6); (b)(7)(C)	(b)(6); @shadowdragonfederal.com (202)207-(b)(6); (b)(7)(C)	(b)(4)	
Atlantic Data Forensics	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C) @atlanticdf.com (410)218-(b)(6);	(b)(4)	
ECS Federal	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C) @ecstech.com (910)322-(b)(6);		No Response
SEALING TECHNOLOGIES	(b)(6);	(b)(6); @sealingtech.org (443)537-(b)(6);	(b)(4)	DUNS: (b)(7)(E)

VI. SUPPORTING DOCUMENTATION

The following supporting documentation is attached:

☒G-514
☒Market Research Memo
☒Privacy Request/exemption
☐BWS/RRB Review
☒Vendor Estimates
☒SAM Verifications
☒IGCE
☐Urgent Justification Form
☐ITSR Stamp
☐Tech Ops Stamp
☐Branding Approval Email
☐Facilities Approval Email/GSA Letter
☐DHS Form 511 – New Request for MFD (Multifunctional Device)
☒JOFOC (Justification for Other than Full and Open Competition)
☐Spec Sheet
☒Appendix G Sensitive Information Checklist
☒Other (***Please Explain)***: J&A

(b)(7)(E)

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-(b)(7)(E)
www.dhs.gov/privacy

DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*. For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement[1]:

a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue and DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications);

b) The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

[1] Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: DHS/OPS/PIA-004(d) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update.

DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer. Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review: August 14, 2019

Name of Component: U.S. Immigration and Customs Enforcement

Contact Information: (b)(6); (b)(7)(C) **Acting Privacy Officer, (202) 732-**(b)(6);

Counsel[2] Contact Information: <Please enter the name, e-mail address, and phone number of the Component Counsel who approved the authorities listed below.>

IT System(s) where social media data is stored: General Counsel Electronic Management System (GEMS), Joint Integrity Case Management System (JICMS), Integrated Security Management System (ISMS), Insider Threat Program.

Applicable Privacy Impact Assessment(s) (PIA):

DHS/ICE/PIA-036 – OPLA Case Management System

DHS/ALL/PIA-038 Integrated Security Management System

DHS/ALL/PIA-038(a) Integrated Security Management System

DHS/ALL/PIA-038(b) Integrated Security Management System

DHS/ALL/PIA-038(c) Integrated Security Management System (ISMS) June 2017

DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS) July 2017

DHS-ALL-PIA-052(a) DHS Insider Threat Program - March 2018

Applicable System of Records Notice(s) (SORN):

DHS/ICE-003 – General Counsel Electronic Management System (GEMS)

DHS/ALL-020 – DHS Internal Affairs Records

[2] Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.

DHS/ALL-017 – DHS General Legal Records

DHS/ALL-020 – DHS Internal Affairs Records

DHS/ALL-038 Insider Threat Program System of Records

DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. **Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.**

   As the definition of social media in the DHS Instruction 110-01-001 Privacy Policy for the Operational Use of Social Media (Privacy Policy) is drafted broadly so as to likely include general use of the Internet and as social media technology is ever changing and evolving, this submission addresses ICE's use of the Internet, to include social media as defined in the Privacy Policy.

   ICE uses the Internet, including social media, as defined in the Privacy Policy, for administrative law enforcement purposes in an internal affairs context. This administrative law enforcement use of the Internet, including social media, includes assisting in investigating, gathering evidence, and gathering information on improper or potentially improper activity by ICE or CBP employees or contractors.

(b)(7)(E)

2. **Based on the operational use of social media listed above, please provide the appropriate authorities.**

   - Inspector General Act of 1978, as amended. (Pub. L. 95–452, 92 Stat. 1101 (1978)
   - Homeland Security Act of 2002, as amended, Pub. L. No. 107-296, 116 Stat. 2135 (2002)
   - DHS Management Directive 0810.1, The Office of Inspector General
   - DHS Delegation No. 7030.2, Delegation of Authority to the Assistant Secretary of U.S. Immigration and Customs Enforcement

a) Has Counsel listed above reviewed these authorities for privacy issues and determined that they permit the Program to use social media for the listed operational use?

☒ Yes. ☐ No.

3. Is this use of social media in development or operational?

☐ In development. ☒ Operational. Date first launched: Unknown.

The Internet has been in use at ICE's legacy agencies since it was publicly available.

4. Please attach a copy of the Rules of Behavior that outline the requirements below.

See Memorandum from John Morton, Use of Public and Non-Public Online Information, June 28, 2012.

5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:

a) *Equipment*. Use only government-issued equipment when engaging in the operational use of social media;

☐ Yes. ☒ No. If not, please explain:

The nature of administrative law enforcement investigations may require investigators to use non-government-issued equipment when engaging in investigations. Investigators at times find themselves in rapidly evolving situations in the field that call for the use of adaptive measures. In situations where government-issued equipment is either not available, or is technologically insufficient to perform the required task at hand, investigators may need to rely on non-government-issued equipment. However, ICE is currently working to provide government-issued equipment so as to not require the use of non-government-issued equipment in these circumstances.

b) *Email and accounts*. Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

☐ Yes. ☒ No. If not, please explain:

Because the activities described in Question 1 are for administrative law enforcement purposes in an internal affairs context, the employees who engage in these activities will not identify themselves as ICE or DHS personnel, or law enforcement personnel. This is necessary to ensure the safety of law enforcement personnel, to avoid compromising law enforcement operations, to prevent tipping off individuals who are sought by law enforcement for violations of law, and to prevent disclosing litigation strategy and tactics.

c) *Public interaction*. Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

☒ Yes. ☐ No. If not, please explain:

d) *Privacy settings*. Respect individuals' privacy settings and access only information that is publicly available;

☐ Yes. ☒ No. If not, please explain:

Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into private space. Where legal authority exists, law enforcement personnel may access restricted online information.

e) *PII collection*: Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

☐ Yes. ☒ No. If not, please explain:

The applicable SORNs cited above are all exempted by Final Rules from the Privacy Act (e)(1) requirement (5 U.S.C. § 552a(e)(1)), which normally limits agencies to collecting only information about individuals that is relevant and necessary to accomplish a purpose of the agency required by statute or Executive Order. The exemption from the (e)(1) requirement is necessary to ensure the integrity of law enforcement investigations, as more fully detailed in the Final Rules.

f) *PII safeguards*. Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

☒ Yes. ☐ No. If not, please explain:

g) *Documentation*. Document operational use of social media, including date, site(s) accessed, information collected and how it was used in the same manner as the component would document information collected from any source in the normal course of business.

☐ Yes. ☒ No. If not, please explain:

ICE's rules of behavior state that law enforcement personnel should retain the information they access on the Internet, including social media, if they would have retained that content had it been written on paper. These contents should be preserved in a manner authorized by ICE procedures governing the preservation of electronic

communications.

h) *Training*. Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

☒ Yes. ☐ No. If not, please explain:

Mechanisms are (or will be) in place to verify that users have completed training.

☐ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office:

NAME of the DHS Privacy Office Reviewer: <Please enter name of reviwer.>

DHS Privacy Office Determination

☐ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

☐ Program has not yet met requirements to utilize social media for operational purposes.

- ☐ Program authorities do not authorize operational use of social media.
- ☐ Rules of Behavior do not comply. <Please explain analysis.>
- ☐ Training required.

Additional Privacy compliance documentation is required:

- ☐ A PIA is required.
  - ☐ Covered by existing PIA. <Please include the name and number of PIA here.>
  - ☐ New.
  - ☐ Updated. <Please include the name and number of PIA to be updated here.>
- ☐ A SORN is required:
  - ☐ Covered by existing SORN. <Please include the name and number of SORN here.>
  - ☐ New.
  - ☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

MARKET RESEARCH MEMORANDUM

TO: Contracting Officer/Specialist *(I.E. CONTRACTING OFFICER/SPECIALIST)*

FROM: HSI Intelligence, IESD (b)(6); (b)(7)(C)

SUBJECT:

ShadowDragon Maltigo Licenses

DATE: 4/27/2020

This memorandum is in accordance with Federal Acquisition Regulation (FAR) Part 10.000, which describes the policies and procedures for conducting market research to reach the most suitable approach to acquiring, distributing, and supporting supplies and services. This Part implements requirements of 41 U.S.C. 253a (a) (1), 41 U.S.C. 264b, and 10 U.S.C. 2377.

I. BACKGROUND

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), the largest investigative agency in the U.S. Department of Homeland Security (DHS), protects national security by enforcing the nation's immigration and customs laws. ICE HSI Office of Intelligence (Intel) has a broad and complex public safety mission which is furthered through the collection and sharing of timely and accurate intelligence on illicit trade, travel, and financial activity with a nexus to the United States. Intel leads this agency-wide continuity of operations, emergency response and crisis management to include establishing and maintaining an agency-wide secure data communication connectivity. One of the leading priorities of HSI Intel is to combat criminal activity conducted on or facilitated by the Internet. HSI Intel delivers computer-based technical services to HSI components to support domestic and international investigations into cross-border crimes. HSI Intel is comprised of the Intelligence Analysis Division, Intelligence Collection Division, Intelligence Integration & Emergency Management Division and Intelligence Enterprise Services Division.

II. REQUIREMENT

HSI-INTEL has a requirement on a sole source basis to purchase ShadowDragon cyber investigation tools on a trial basis. Due to rapidly advancing technology and the need to remain

vigilant, HSI-INTEL must continuously identify tools that can enhance and support ICE's law enforcement and intelligence mission.

ShadowDragon SocialNet access is provided through the Maltego application. The platform can be installed on NON-IRMNET laptops currently deployed across the HSI enterprise. This requirement is to allow HSI-Intel access to ShadowDragon SocialNet for a sixty (60) day trial basis.

ShadowDragon develops cyber intelligence solutions that provide threat-related information to organizations, enabling them to stop and attribute targeted actions of malicious actors in the physical or digital world. These solutions are achieved through monitoring and analyzing data from proprietary threat databases, the Internet and the dark web. ShadowDragon is used to by hundreds of private businesses, intelligence and law enforcement organizations globally.

ShadowDragon, will allow HSI-INTEL access to the tools, identified below, in support of its investigative mission(s):

SocialNet is a unique interactive data mining tool that renders directed graphs for link analysis. The results are visualized in minutes to reveal detailed 1 to 1 correlation as well as larger networks of associates. Features include:

- Easy, fast, and reliable visualization of people's profile information and relationships
- Search 60+ social networking sites and other account based online entities.
- Complete multiple queries in minutes, which would take hours or days to complete manually.
- Visualize 1 to 1 correlations as well as multiple relationships and networks of people into the 1000s of records.
- Reliable and accurate results with a proprietary data collection/query methodology that has been refined over five years and is continually updated.

III. DELIVERY/PERFORMANCE TIME

Need by date: 9/1/2020
Base Period of Performance (POP) dates: *From* 9/7/2020 *To* 9/6/2021

Click the link to see if the need is "Urgent":
http://intranet.ice.dhs.gov/sites/oaq/resources/palt.htm

☒No
☐Yes (Urgent Justification Form Required)

IV. METHODOLOGY OF MARKET RESEARCH

The results of market research have determined that the Government's needs can be met by:

☐Items of a type customarily available in the commercial marketplace;
☐Items of a type customarily available in the commercial marketplace with modifications; or
☒Items used exclusively for governmental purposes.

The following methods were utilized to conduct Market Research:

☐FedBizOpps Sources Sought Synopsis (https://www.fbo.gov/)
☒GSA/FSS (GSA Advantage)
https://www.gsaadvantage.gov/advantage/main/start_page.do)
☐Unicor (http://www.unicor.gov/)
☐JWOD/AbilityOne (http://www.abilityone.gov/)
☒SAM (https://www.sam.gov/portal/public/SAM/)
☐Previous purchases of similar/identical items
☐Internet
☐Contacted SBA (http://www.sba.gov/)
☒Firstsource II (http://mgmt-opo-sp.dhs.gov/sites/epic/Pages/FirstSource%20II.aspx)
☒Other (***Please Explain)***: Single Source
☒Other Strategic Source (BPA, IDIQ, etc.)

Ex: http://dhsconnect.dhs.gov/org/comp/mgmt/cpo/oss/Pages/StrategicSourcing.aspx)

Ex: TacCom Motorola HSSS01-12-D-0002)

V. SUMMARY OF MARKET RESEARCH

HSI Intel conducted Market Research to identify and obtain pricing estimates from each of the First Source II - HUBZone Socioeconomic Category vendors and the SB Socio Economic Category vendors to receive the follow summary quotes.

The apparent fair market value based on the Market Research conducted and the cost estimate received is $(b)(6); (b)(7)(C) for 100 licenses annually.

Vendor Name	Vendor POC	Vendor Info	Estimated Cost	Comments
Shadow Dragon	(b)(6); (b)(7)(C)	(b)(6); @shadowdragonfederal.com	$(b)(6);	

		(202)207-(b)(6); (b)(7)(C)		
Atlantic Data Forensics	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C) @atlanticdf.com (410)218-(b)(6);		
ECS Federal	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C) @ecstech.com (910)322-(b)(6);		
SEALING TECHNOLOGIES	(b)(6);	(b)(6); @sealingtech.org (443)537-(b)(6);		DUNS: (b)(6); (b)(7)(C)

VI. SUPPORTING DOCUMENTATION

The following supporting documentation is attached:

☒G-514
☒Market Research Memo
☒Privacy Request/exemption
☐BWS/RRB Review
☒Vendor Estimates
☒SAM Verifications
☒IGCE
☐Urgent Justification Form
☐ITSR Stamp
☐Tech Ops Stamp
☐Branding Approval Email
☐Facilities Approval Email/GSA Letter
☐DHS Form 511 – New Request for MFD (Multifunctional Device)
☒JOFOC (Justification for Other than Full and Open Competition)
☐Spec Sheet
☒Appendix G Sensitive Information Checklist
☒Other (***Please Explain)***: J&A

REQUISITION — MATERIALS-SUPPLIES-EQUIPMENT

SEE INSTRUCTIONS ON REVERSE

1. NUMBER: 192121IHQRQN00041
2. DATE: 12-JUL-2021
3. ACTIVITY SYMBOL: See Attachment A

4. TO: NAME AND ADDRESS -- PROCUREMENT SECTION (OR STOREROOM)
DEPARTMENT OF HOMELAND SECURITY
IMMIGRATION AND CUSTOMS ENFORCEMENT
OFFICE OF ACQUISITION MANAGEMENT(OAQ)
7701 N. STEMMONS FRWY
DALLAS, TEXAS 75247

5. FROM: NAME AND ADDRESS -- REQUISITIONER
ICE-INTEL
(b)(6);
(b)(6); @ICE.DHS.GOV
202-732-(b)(
500 12TH STREET SW
WASHINGTON, DC 20536
US

STOCK NUMBER	DESCRIPTION OF ARTICLE (MAKE, MODEL, TYPE, SIZE, COLOR, MFGR., ETC)	QUANTITY	UNIT	COST		ACTION CODE
				UNIT PRICE	AMOUNT	
6	7	8	9	10	11	12
	SOCIALNET IDENTITY MANAGEMENT SECURED LINK ANALYSIS BUNDLED WITH MALTEGO CLASSIC - ANNUAL SUBSCRIPTION	1	EA	(b)(6);	(b)(6);	

Justification:

SOFTWARE LICENSE PROCUREMENT FOR SOCIALNET+MALTEGO. PCOR (b)(6); (b)(7)(C) /APOC: (b)(6); (b)(6);

Recommended Vendor:

No Recommended Vendor

13. SIGNATURE OF APPROVING OFFICIAL	Date	14. TITLE OF APPROVING OFFICIAL
(b)(6); (b)(7)(C)	12-JUL-2021	SUPVY MGMT & PROG ANAL

24. SIGNATURE OF FUNDING OFFICIAL	Date	25. TITLE OF FUNDING OFFICIAL	15. TOTAL
(b)(6);	12-JUL-2021	MGMT & PROG ANAL	(b)(6);

16. KEY TO ACTION CODE			
S	SUBSTITUTE ITEM	2	CANCELLED--NOT STOCKED
B	BACK ORDERED	3	CANCELLED--NOT ABLE TO IDENTIFY
D	PURCHASED FOR DIRECT SHIPMENT	0	OTHER -- AS INDICATED
1	CANCELLED--STOCK EXHAUSTED		

PROCUREMENT SECTION (OR STOREROOM)

17. DATE RECEIVED	19. PURCHASE ORDER	
	DATE	NUMBER
18. APPROVED		

I CERTIFY THAT THE ABOVE ARTICLES -- COLUMNS 3, 9 AND 12 - HAVE BEEN RECEIVED.

20. LOCATION	21. DATE	22. SIGNATURE	23. TITLE

United States Department Of Homeland Security
Immigration And Customs Enforcement
FORM G-514 (REV. 8-1-5

INSTRUCTIONS

Use

Use Form G-514 - continued on Form G-514.1 -- To requisition materials, supplies, and equipment through the Procurement section of the Regional (or Central) Office; or from a Service-operated Storeroom.

Copies - Distribution

Prepared by requistioner in an original and two copies, sending original (white) and Copy 1 (pink) to: Procurement Section (or Storeroom), and retaining Copy 2 (green). Procurement Section (or Storeroom) shall, as a rule, pack Copy 1 with shipment, or return it to requisitioner with appropriate advice.

Entries

By requisitioner:

1. Number consecutively, beginning with number one each fiscal year, and prefix with alphabetic location symbol and last two digits of fiscal year (e.g., MIA-58-1, MIA-58-2, MIA-58-3, etc., MIA-59-1, MIA-59-2, MIA-59-3, etc.). Number continuation sheets with numerical suffix(e.g., MIA-58-1.1, MIA-58-1.2, MIA-58-1.3, etc).
2. Enter date of preparation.
3. Enter numerical symbol of activity which will benefit from use of articles.
4. Enter name and address of Procurement section (or Storeroom)(e.g., Procurement Section, Immigration and Naturalization Service, Richmond, VA).
5. Enter full name, title, and address so that shipping label may be prepared without reference to address directory. If consignee is other than requisitioner, enter shipping instructions under Entry 7.
6. Enter form numbers; stock number shown in "Stores Stock Catalog" and "Federal Supply Schedules."
7. Enter full description of article; attach sketches, plans, samples, etc. If consignee is other than requisitioner, enter shipping instructions.
8. Enter issue - unit quantity.
9. Enter unit of issue (e.g., each, doz., C, gross, ream, M; lb., cwt, ton: bag, ball, bbl., bot., box, can, pkg., roll, tube; pt., qt., gal., etc.)
13. Signature of approving official.
14. Enter title of approving official.
24. Signature of funding official.
25. Enter title of funding official.

By Procurement Section (or Storeroom):

10. Enter unit price.
11. Enter product of Entries 8 and 10.
12. Enter symbol of action taken. See Entry 16.
15. Enter total of amounts under Entry 11.
17. Enter date requisition received.
18. Signature of approving officer.
19. Enter, if issued, date and number of purchase order.

By consignee:

20. Enter address - city and state.
21. Enter date shipment received.
22. Signature of employee authorized to accept delivery.
23. Enter title of receiving employee.

Form G-514

REQUISITION - MATERIALS-SUPPLIES-EQUIPMENT
Activity Symbols
ATTACHMENT A

REQUISITION NUMBER: **192121IHQRQN00041**

Item No.	Contract No.	Task Ord No.	Project	Task	Fund	Program	Organization	Object	UDF	Amount
1			INTDIV4	LIC	D4	88-00-00-000	70-08-0002-02-00-00-00	GE-31-19-00	000000	$(b)(6);

APPROPRIATION SYMBOL CROSSWALK:

FUND	FY	TAS	TITLE	AMOUNT
D4	2021	7010540		(b)(6);

United States Department Of Homeland Security
Immigration And Customs Enforcement
FORM G-514 (REV. 8-1-5

REQUISITION — MATERIALS-SUPPLIES-EQUIPMENT

** Amendment 1 of 1 **

SEE INSTRUCTIONS ON REVERSE

1. NUMBER: 192121IHQRQN00041

2. DATE: 05-AUG-2021

3. ACTIVITY SYMBOL: See Attachment A

4. TO: NAME AND ADDRESS -- PROCUREMENT SECTION (OR STOREROOM)
DEPARTMENT OF HOMELAND SECURITY
IMMIGRATION AND CUSTOMS ENFORCEMENT
OFFICE OF ACQUISITION MANAGEMENT(OAQ)
7701 N. STEMMONS FRWY
DALLAS, TEXAS 75247

FFMS

5. FROM: NAME AND ADDRESS -- REQUISITIONER
ICE-INTEL
(b)(6);
(b)(6); @ICE.DHS.GOV
202-732-(b)(
500 12TH STREET SW
WASHINGTON, DC 20536
US

STOCK NUMBER	DESCRIPTION OF ARTICLE (MAKE, MODEL, TYPE, SIZE, COLOR, MFGR., ETC)	QUANTITY	UNIT	COST		ACTION CODE
				UNIT PRICE	AMOUNT	
6	7	8	9	10	11	12
	SOCIALNET IDENTITY MANAGEMENT SECURED LINK ANALYSIS BUNDLED WITH MALTEGO CLASSIC - ANNUAL SUBSCRIPTION	1	EA	(b)(6);	(b)(6);	

ITSR
08/09/2021
REQ0421024
IT approval not required
GM

Justification:

SOFTWARE LICENSE PROCUREMENT FOR SOCIALNET+MALTEGO. PCOR (b)(6); ACOR (b)(6); (b)(6); (b)(7)(C)

Recommended Vendor:

No Recommended Vendor

13. SIGNATURE OF APPROVING OFFICIAL	Date	14. TITLE OF APPROVING OFFICIAL
(b)(6); (b)(7)(C)	05-AUG-2021	SUPVY MGMT & PROG ANAL

24. SIGNATURE OF FUNDING OFFICIAL	Date	25. TITLE OF FUNDING OFFICIAL	15. TOTAL
(b)(6);	05-AUG-2021	MGMT & PROG ANAL	(b)(6);

16. KEY TO ACTION CODE				PROCUREMENT SECTION (OR STOREROOM)		
S	SUBSTITUTE ITEM	2	CANCELLED--NOT STOCKED	17. DATE RECEIVED	19. PURCHASE ORDER DATE	NUMBER
B	BACK ORDERED	3	CANCELLED--NOT ABLE TO IDENTIFY			
D	PURCHASED FOR DIRECT SHIPMENT	0	OTHER -- AS INDICATED	18. APPROVED		
1	CANCELLED--STOCK EXHAUSTED					

I CERTIFY THAT THE ABOVE ARTICLES -- COLUMNS 3, 9 AND 12 - HAVE BEEN RECEIVED.

20. LOCATION	21. DATE	22. SIGNATURE	23. TITLE

1. Agency and Contracting Activity.

The Department of Homeland Security, U.S. Immigration and Customs Enforcement, Office of Acquisition Management, prepared this justification for an exception to fair opportunity on behalf of Homeland Security Investigations (HSI), Office of Intelligence (INTEL).

2. Nature and/or description of the item/service being procured and anticipated cost:

(a) Type of action: Firm-fixed price contract

(b) Amount the current J&A is justifying: $(b)(6); (b)(7)(C)

(c) Brief Description: OAQ intends to procure brand-name ShadowDragon SocialNet licenses through DHS First-Source II IDIQ contract. Although, it is offered by multiple authorized resellers, the company listed below is the only developer of this particular brand-name software.

ShadowDragon Federal, LLC
1505 E. 16th St.
Cheyenne, WY 82001

3. Description of Supplies/Services.

HSI-INTEL has a requirement on a brand-name basis to purchase ShadowDragon SocialNet cyber investigation tools as described in the table below. ShadowDragon develops cyber intelligence solutions that provide threat-related information to organizations, enabling them to stop and attribute targeted actions of malicious actors in the physical or digital world. These solutions are achieved through monitoring and analyzing data from proprietary threat databases, the internet, and the dark web. ShadowDragon is used by hundreds of private businesses, intelligence and law enforcement organizations globally. SocialNet is a unique interactive data mining tool that renders directed graphs for link analysis. The results are visualized in minutes to reveal detailed 1 to 1 correlation as well as larger networks of associates.

Required features include:

- Fast, and reliable visualization of people's profile information and relationships
- Search 100+ social networking sites and other account based online entities.
- Visualize 1 to 1 correlations as well as multiple relationships and networks of people into the 1000s of records.
- Reliable and accurate results
- Data collection/query methodology that is continually updated.

U.S. Immigration and Customs Enforcement

JUSTIFICATION FOR EXCEPTION TO FAIR OPPORTUNITY
BRAND NAME: FAR 16.505(a)(4) and 16.505(b)(2)(ii)

Part Number	Description	Quantity	Unit Price	Total Price
SD-FED-SocNet-250-MaltegoBundle	SocialNet Identity Management Secured Link Analysis Bundled With Maltego Classic - 250 Queries/Day 12 Month Subscription	100	$(b)(6);	$(b)(6); (b)(7)(C)

4. Statutory Exception and rationale for its use:

Exception:
Pursuant to 41 U.S.C. 4106(c)(2) as implemented by FAR 16.505(a)(4) the brand name items/items peculiar to one manufacturer are essential to the Government's requirements and market research indicates other companies' similar products, or products lacking the particular feature, do not meet, or cannot be modified to meet, the agency's needs.

Rationale:
OAQ intends to procure a brand name specification for ShadowDragon SocialNet in accordance with FAR 16.505(a)(4) based on the statutory exception listed above. HSI-INTEL conducted market research on the following alternate products:(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

5. Pre-award synopsis of this Brand Name JEFO exceeding $(b)(6); : Select one (1) of the options below:

☐ ICE intends to provide this justification and supporting documentation along with the solicitation to all contract awardees pursuant to FAR 16.505(a)(4)(iii)(A)(2).

☒ ICE does not intend provide this justification and supporting documentation along with the solicitation to all contract awardees pursuant to a synopsis exception under FAR 16.505(a)(4)(iii)(C).

☐ Not applicable. The dollar value of this J&A is less than $(b)(6);

6. Determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable.

The contracting officer determines that the anticipated price(s) will be fair and reasonable based on price competition. This will be competed on DHS First Source II and it is anticipated that multiple offers will be received from the vendors on DHS First Source II. Additionally, the pricing will be compared to the Independent Government Cost Estimate (IGCE) which was derived by querying several re-sellers and averaging their pricing.

7. Any other facts supporting the justification.

None.

8. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

ICE will continue to monitor available products to determine if alternate products will satisfy future requirements. However, to increase competition, OAQ will seek and solicit as many authorized resellers of the ShadowDragon SocialNet tool as possible.

9. <u>Post-award</u> publishing of this Brand Name JEFO, after the order has been placed. Select one of the items below if this JEFO exceeds $(b)(6); (simplified acquisition threshold):

☐ ICE intends to post this JEFO on System for Award Management (SAM) with the solicitation pursuant to FAR 16.505(b)(2)(ii)(D).

☒ ICE does not intend to post this JEFO on System for Award Management (SAM) with the solicitation pursuant to FAR 16.505(b)(2)(ii)(D)(5).

☐ Not applicable. The dollar value of this J&A does not exceed $(b)(6);

MARKET RESEARCH MEMORANDUM

TO: Contracting Officer/Specialist *(I.E. CONTRACTING OFFICER/SPECIALIST)*

FROM: HSI Intelligence, IESD (b)(6); (b)(7)(C)

SUBJECT:

ShadowDragon SocialNet/Maltigo Licenses

DATE: 5/11/2021

This memorandum is in accordance with Federal Acquisition Regulation (FAR) Part 10.000, which describes the policies and procedures for conducting market research to reach the most suitable approach to acquiring, distributing, and supporting supplies and services. This Part implements requirements of 41 U.S.C. 253a (a) (1), 41 U.S.C. 264b, and 10 U.S.C. 2377.

I. BACKGROUND

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), the largest investigative agency in the U.S. Department of Homeland Security (DHS), protects national security by enforcing the nation's immigration and customs laws. ICE HSI Office of Intelligence (Intel) has a broad and complex public safety mission which is furthered through the collection and sharing of timely and accurate intelligence on illicit trade, travel, and financial activity with a nexus to the United States. Intel leads this agency-wide continuity of operations, emergency response and crisis management to include establishing and maintaining an agency-wide secure data communication connectivity. One of the leading priorities of HSI Intel is to combat criminal activity conducted on or facilitated by the Internet. HSI Intel delivers computer-based technical services to HSI components to support domestic and international investigations into cross-border crimes. HSI Intel is comprised of the Intelligence Analysis Division, Intelligence Collection Division, Intelligence Integration & Emergency Management Division and Intelligence Enterprise Services Division.

II. REQUIREMENT

HSI-INTEL has a requirement on a sole source basis to purchase ShadowDragon

SocialNet/Maltego cyber investigation tools on a trial basis. Due to rapidly advancing technology and the need to remain vigilant, HSI-INTEL must continuously identify tools that can enhance and support ICE's law enforcement and intelligence mission.

SocialNet access is provided through the Maltego application. The platform can be installed on NON-IRMNET laptops currently deployed across the HSI enterprise. This requirement is to allow HSI-Intel access to ShadowDragon SocialNet/Maltego Classic for on year.

SocialNet develops cyber intelligence solutions that provide threat-related information to organizations, enabling them to stop and attribute targeted actions of malicious actors in the physical or digital world. These solutions are achieved through monitoring and analyzing data from proprietary threat databases, the Internet and the dark web. SocialNet is used to by hundreds of private businesses, intelligence and law enforcement organizations globally.

ShadowDragon, will allow HSI-INTEL access to the tools, identified below, in support of its investigative mission(s):

SocialNet is a unique interactive data mining tool that renders directed graphs for link analysis. The results are visualized in minutes to reveal detailed 1 to 1 correlation as well as larger networks of associates. Features include:

- Easy, fast, and reliable visualization of people's profile information and relationships
- Search 60+ social networking sites and other account based online entities.
- Complete multiple queries in minutes, which would take hours or days to complete manually.
- Visualize 1 to 1 correlations as well as multiple relationships and networks of people into the 1000s of records.
- Reliable and accurate results with a proprietary data collection/query methodology that has been refined over five years and is continually updated.

III. DELIVERY/PERFORMANCE TIME

Need by date: 9/1/2020
Base Period of Performance (POP) dates: *From* 9/7/2020 *To* 9/6/2021

Click the link to see if the need is "Urgent":
http://intranet.ice.dhs.gov/sites/oaq/resources/palt.htm

☒No
☐Yes (Urgent Justification Form Required)

IV. METHODOLOGY OF MARKET RESEARCH

The results of market research have determined that the Government's needs can be met by:

☐Items of a type customarily available in the commercial marketplace;
☐Items of a type customarily available in the commercial marketplace with modifications; or
☒Items used exclusively for governmental purposes.

The following methods were utilized to conduct Market Research:

☐FedBizOpps Sources Sought Synopsis (https://www.fbo.gov/)
☒GSA/FSS (GSA Advantage)
https://www.gsaadvantage.gov/advantage/main/start_page.do)
☐Unicor (http://www.unicor.gov/)
☐JWOD/AbilityOne (http://www.abilityone.gov/)
☒SAM (https://www.sam.gov/portal/public/SAM/)
☐Previous purchases of similar/identical items
☐Internet
☐Contacted SBA (http://www.sba.gov/)
☒Firstsource II (http://mgmt-opo-sp.dhs.gov/sites/epic/Pages/FirstSource%20II.aspx)
☒Other (***Please Explain)***: Single Source
☒Other Strategic Source (BPA, IDIQ, etc.)

Ex: http://dhsconnect.dhs.gov/org/comp/mgmt/cpo/oss/Pages/StrategicSourcing.aspx)

Ex: TacCom Motorola HSSS01-12-D-0002)

V. SUMMARY OF MARKET RESEARCH

HSI Intel conducted Market Research to identify and obtain pricing estimates from each of the First Source II - HUBZone Socioeconomic Category vendors and the SB Socio Economic Category vendors to receive the follow summary quotes.

The apparent fair market value based on the Market Research conducted and the cost estimate received is (b)(4)

Vendor Name	Vendor POC	Vendor Info	Estimated Cost	Comments
Shadow Dragon	(b)(6); (b)(7)(C)	(b)(6); @shadowdragonfederal.com	(b)(4)	

		(202)207-(b)(6); (b)(7)(C)		
Atlantic Data Forensics	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C) @atlanticdf.com (410)218-(b)(6);		
ECS Federal		(b)(6); (b)(7)(C) @ecstech.com (910)322(b)(6);		
SEALING TECHNOLOGIES		(b)(6); (b)(7)(C) sealingtech.org (443)537(b)(6);		DUNS: 078491625

VI. SUPPORTING DOCUMENTATION

The following supporting documentation is attached:

☒G-514
☒Market Research Memo
☒Privacy Request/exemption
☐BWS/RRB Review
☒Vendor Estimates
☒SAM Verifications
☒IGCE
☐Urgent Justification Form
☐ITSR Stamp
☐Tech Ops Stamp
☐Branding Approval Email
☐Facilities Approval Email/GSA Letter
☐DHS Form 511 – New Request for MFD (Multifunctional Device)
☒JOFOC (Justification for Other than Full and Open Competition)
☐Spec Sheet
☒Appendix G Sensitive Information Checklist
☒Other (***Please Explain)***: J&A

MARKET RESEARCH MEMORANDUM

TO: Contracting Officer/Specialist *(I.E. CONTRACTING OFFICER/SPECIALIST)*

FROM: HSI Intelligence, IESD (b)(6); (b)(7)(C)

SUBJECT:

ShadowDragon SocialNet/Maltigo Licenses

DATE: 5/11/2021

This memorandum is in accordance with Federal Acquisition Regulation (FAR) Part 10.000, which describes the policies and procedures for conducting market research to reach the most suitable approach to acquiring, distributing, and supporting supplies and services. This Part implements requirements of 41 U.S.C. 253a (a) (1), 41 U.S.C. 264b, and 10 U.S.C. 2377.

I. BACKGROUND

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), the largest investigative agency in the U.S. Department of Homeland Security (DHS), protects national security by enforcing the nation's immigration and customs laws. ICE HSI Office of Intelligence (Intel) has a broad and complex public safety mission which is furthered through the collection and sharing of timely and accurate intelligence on illicit trade, travel, and financial activity with a nexus to the United States. Intel leads this agency-wide continuity of operations, emergency response and crisis management to include establishing and maintaining an agency-wide secure data communication connectivity. One of the leading priorities of HSI Intel is to combat criminal activity conducted on or facilitated by the Internet. HSI Intel delivers computer-based technical services to HSI components to support domestic and international investigations into cross-border crimes. HSI Intel is comprised of the Intelligence Analysis Division, Intelligence Collection Division, Intelligence Integration & Emergency Management Division and Intelligence Enterprise Services Division.

II. REQUIREMENT

HSI-INTEL has a requirement on a sole source basis to purchase ShadowDragon

SocialNet/Maltego cyber investigation tools on a trial basis. Due to rapidly advancing technology and the need to remain vigilant, HSI-INTEL must continuously identify tools that can enhance and support ICE's law enforcement and intelligence mission.

SocialNet access is provided through the Maltego application. The platform can be installed on NON-IRMNET laptops currently deployed across the HSI enterprise. This requirement is to allow HSI-Intel access to ShadowDragon SocialNet/Maltego Classic for on year.

SocialNet develops cyber intelligence solutions that provide threat-related information to organizations, enabling them to stop and attribute targeted actions of malicious actors in the physical or digital world. These solutions are achieved through monitoring and analyzing data from proprietary threat databases, the Internet and the dark web. SocialNet is used to by hundreds of private businesses, intelligence and law enforcement organizations globally.

ShadowDragon, will allow HSI-INTEL access to the tools, identified below, in support of its investigative mission(s):

SocialNet is a unique interactive data mining tool that renders directed graphs for link analysis. The results are visualized in minutes to reveal detailed 1 to 1 correlation as well as larger networks of associates. Features include:

- Easy, fast, and reliable visualization of people's profile information and relationships
- Search 60+ social networking sites and other account based online entities.
- Complete multiple queries in minutes, which would take hours or days to complete manually.
- Visualize 1 to 1 correlations as well as multiple relationships and networks of people into the 1000s of records.
- Reliable and accurate results with a proprietary data collection/query methodology that has been refined over five years and is continually updated.

III. DELIVERY/PERFORMANCE TIME

Need by date: 9/1/2020
Base Period of Performance (POP) dates: *From* 9/7/2020 *To* 9/6/2021

Click the link to see if the need is "Urgent":
http://intranet.ice.dhs.gov/sites/oaq/resources/palt.htm

☒No
☐Yes (Urgent Justification Form Required)

IV. METHODOLOGY OF MARKET RESEARCH

The results of market research have determined that the Government's needs can be met by:

☐Items of a type customarily available in the commercial marketplace;
☐Items of a type customarily available in the commercial marketplace with modifications; or
☒Items used exclusively for governmental purposes.

The following methods were utilized to conduct Market Research:

☐FedBizOpps Sources Sought Synopsis (https://www.fbo.gov/)
☒GSA/FSS (GSA Advantage)
https://www.gsaadvantage.gov/advantage/main/start_page.do)
☐Unicor (http://www.unicor.gov/)
☐JWOD/AbilityOne (http://www.abilityone.gov/)
☒SAM (https://www.sam.gov/portal/public/SAM/)
☐Previous purchases of similar/identical items
☐Internet
☐Contacted SBA (http://www.sba.gov/)
☒Firstsource II (http://mgmt-opo-sp.dhs.gov/sites/epic/Pages/FirstSource%20II.aspx)
☒Other (***Please Explain)***: Single Source
☒Other Strategic Source (BPA, IDIQ, etc.)

Ex: http://dhsconnect.dhs.gov/org/comp/mgmt/cpo/oss/Pages/StrategicSourcing.aspx)

Ex: TacCom Motorola HSSS01-12-D-0002)

V. SUMMARY OF MARKET RESEARCH

HSI Intel conducted Market Research to identify and obtain pricing estimates from each of the First Source II - HUBZone Socioeconomic Category vendors and the SB Socio Economic Category vendors to receive the follow summary quotes.

The apparent fair market value based on the Market Research conducted and the cost estimate received is $290,000.00 for 100 licenses annually.

Vendor Name	Vendor POC	Vendor Info	Estimated Cost	Comments
Shadow Dragon	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C) @shadowdragonfederal.com	(b)(4)	

		(202)207-(b)(6); (b)(7)(C)		
Atlantic Data Forensics	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C) @atlanticdf.com (410)218-(b)(6); (b)(7)(C)		
ECS Federal		(b)(6); (b)(7)(C) @ecstech.com (910)322(b)(6);		
SEALING TECHNOLOGIES		(b)(6); (b)(7)(C) @sealingtech.org (443)537-(b)(6); (b)(7)(C)		DUNS: 078491625

VI. SUPPORTING DOCUMENTATION

The following supporting documentation is attached:

☒G-514
☒Market Research Memo
☒Privacy Request/exemption
☐BWS/RRB Review
☒Vendor Estimates
☒SAM Verifications
☒IGCE
☐Urgent Justification Form
☐ITSR Stamp
☐Tech Ops Stamp
☐Branding Approval Email
☐Facilities Approval Email/GSA Letter
☐DHS Form 511 – New Request for MFD (Multifunctional Device)
☒JOFOC (Justification for Other than Full and Open Competition)
☐Spec Sheet
☒Appendix G Sensitive Information Checklist
☒Other (***Please Explain)***: J&A

MARKET RESEARCH MEMORANDUM

TO: Contracting Officer/Specialist *(I.E. CONTRACTING OFFICER/SPECIALIST)*

FROM: HSI Intelligence, IESD (b)(6); (b)(7)(C)

SUBJECT:

ShadowDragon Maltigo Licenses

DATE: 4/27/2020

This memorandum is in accordance with Federal Acquisition Regulation (FAR) Part 10.000, which describes the policies and procedures for conducting market research to reach the most suitable approach to acquiring, distributing, and supporting supplies and services. This Part implements requirements of 41 U.S.C. 253a (a) (1), 41 U.S.C. 264b, and 10 U.S.C. 2377.

I. BACKGROUND

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), the largest investigative agency in the U.S. Department of Homeland Security (DHS), protects national security by enforcing the nation's immigration and customs laws. ICE HSI Office of Intelligence (Intel) has a broad and complex public safety mission which is furthered through the collection and sharing of timely and accurate intelligence on illicit trade, travel, and financial activity with a nexus to the United States. Intel leads this agency-wide continuity of operations, emergency response and crisis management to include establishing and maintaining an agency-wide secure data communication connectivity. One of the leading priorities of HSI Intel is to combat criminal activity conducted on or facilitated by the Internet. HSI Intel delivers computer-based technical services to HSI components to support domestic and international investigations into cross-border crimes. HSI Intel is comprised of the Intelligence Analysis Division, Intelligence Collection Division, Intelligence Integration & Emergency Management Division and Intelligence Enterprise Services Division.

II. REQUIREMENT

HSI-INTEL has a requirement on a sole source basis to purchase ShadowDragon cyber investigation tools on a trial basis. Due to rapidly advancing technology and the need to remain

vigilant, HSI-INTEL must continuously identify tools that can enhance and support ICE's law enforcement and intelligence mission.

ShadowDragon SocialNet access is provided through the Maltego application. The platform can be installed on NON-IRMNET laptops currently deployed across the HSI enterprise. This requirement is to allow HSI-Intel access to ShadowDragon SocialNet for a sixty (60) day trial basis.

ShadowDragon develops cyber intelligence solutions that provide threat-related information to organizations, enabling them to stop and attribute targeted actions of malicious actors in the physical or digital world. These solutions are achieved through monitoring and analyzing data from proprietary threat databases, the Internet and the dark web. ShadowDragon is used to by hundreds of private businesses, intelligence and law enforcement organizations globally.

ShadowDragon, will allow HSI-INTEL access to the tools, identified below, in support of its investigative mission(s):

SocialNet is a unique interactive data mining tool that renders directed graphs for link analysis. The results are visualized in minutes to reveal detailed 1 to 1 correlation as well as larger networks of associates. Features include:

- Easy, fast, and reliable visualization of people's profile information and relationships
- Search 60+ social networking sites and other account based online entities.
- Complete multiple queries in minutes, which would take hours or days to complete manually.
- Visualize 1 to 1 correlations as well as multiple relationships and networks of people into the 1000s of records.
- Reliable and accurate results with a proprietary data collection/query methodology that has been refined over five years and is continually updated.

III. DELIVERY/PERFORMANCE TIME

Need by date: 9/1/2020
Base Period of Performance (POP) dates: *From* 9/7/2020 *To* 9/6/2021

Click the link to see if the need is "Urgent":
http://intranet.ice.dhs.gov/sites/oaq/resources/palt.htm

☒No
☐Yes (Urgent Justification Form Required)

IV. METHODOLOGY OF MARKET RESEARCH

The results of market research have determined that the Government's needs can be met by:

☐Items of a type customarily available in the commercial marketplace;
☐Items of a type customarily available in the commercial marketplace with modifications; or
☒Items used exclusively for governmental purposes.

The following methods were utilized to conduct Market Research:

☐FedBizOpps Sources Sought Synopsis (https://www.fbo.gov/)
☒GSA/FSS (GSA Advantage)
https://www.gsaadvantage.gov/advantage/main/start_page.do)
☐Unicor (http://www.unicor.gov/)
☐JWOD/AbilityOne (http://www.abilityone.gov/)
☒SAM (https://www.sam.gov/portal/public/SAM/)
☐Previous purchases of similar/identical items
☐Internet
☐Contacted SBA (http://www.sba.gov/)
☒Firstsource II (http://mgmt-opo-sp.dhs.gov/sites/epic/Pages/FirstSource%20II.aspx)
☒Other (***Please Explain)***: Single Source
☒Other Strategic Source (BPA, IDIQ, etc.)

Ex: http://dhsconnect.dhs.gov/org/comp/mgmt/cpo/oss/Pages/StrategicSourcing.aspx)

Ex: TacCom Motorola HSSS01-12-D-0002)

V. SUMMARY OF MARKET RESEARCH

HSI Intel conducted Market Research to identify and obtain pricing estimates from each of the First Source II - HUBZone Socioeconomic Category vendors and the SB Socio Economic Category vendors to receive the follow summary quotes.

The apparent fair market value based on the Market Research conducted and the cost estimate received is (b)(4)

Vendor Name	Vendor POC	Vendor Info	Estimated Cost	Comments
Shadow Dragon	(b)(6); (b)(7)(C)	(b)(6); @shadowdragonfederal.com	(b)(4)	

		(202)207-(b)(6); (b)(7)(C)		
Atlantic Data Forensics	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C) @atlanticdf.com (410)218(b)(6);		
ECS Federal	(b)(6); (b)(7)(C)	(b)(6); (b)(7)(C) @ecstech.com (910)32(b)(6);		
SEALING TECHNOLOGIES	(b)(6);	(b)(6); @sealingtech.org (443)537(b)(6);		DUNS: 078491625

VI. SUPPORTING DOCUMENTATION

The following supporting documentation is attached:

☒G-514
☒Market Research Memo
☒Privacy Request/exemption
☐BWS/RRB Review
☒Vendor Estimates
☒SAM Verifications
☒IGCE
☐Urgent Justification Form
☐ITSR Stamp
☐Tech Ops Stamp
☐Branding Approval Email
☐Facilities Approval Email/GSA Letter
☐DHS Form 511 – New Request for MFD (Multifunctional Device)
☒JOFOC (Justification for Other than Full and Open Competition)
☐Spec Sheet
☒Appendix G Sensitive Information Checklist
☒Other (***Please Explain)***: J&A

U.S. Immigration and Customs Enforcement

STATEMENT OF WORK

Shadow Dragon SocialNet w/Maltigo

JULY 2021

Homeland Security Investigations (HSI)

DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS
OFFICE OF INTELLIGENCE (INTEL)
STATEMENT OF WORK
For SHADOW DRAGON
SOCIALNET w/MALTIGO
Date: 7/14/2021

1. GENERAL

Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Office of Intelligence (INTEL) has a broad and complex public safety mission which is furthered through the collection and sharing of timely and accurate intelligence on illicit trade, travel, and financial activity with a nexus to the United States.

2. BACKGROUND

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), the largest investigative agency in the U.S. Department of Homeland Security (DHS), protects national security by enforcing the nation's immigration and customs laws. ICE HSI Office of Intelligence (Intel) has a broad and complex public safety mission which is furthered through the collection and sharing of timely and accurate intelligence on illicit trade, travel, and financial activity with a nexus to the United States. Intel leads this agency-wide continuity of operations, emergency response and crisis management to include establishing and maintaining an agency-wide secure data communication connectivity. One of the leading priorities of HSI Intel is to combat criminal activity conducted on or facilitated by the Internet. HSI Intel delivers computer-based technical services to HSI components to support domestic and international investigations into cross-border crimes. HSI Intel is comprised of the Intelligence Analysis Division, Intelligence Collection Division, Intelligence Integration & Emergency Management Division, and Intelligence Enterprise Services Division.

3. SCOPE

HSI-INTEL has a requirement on a Brand Name sole source basis to purchase ShadowDragon cyber investigation SocialNet through the Maltego platform tool for on (1) base year. Due to rapidly advancing technology and the need to remain vigilant, HSI-INTEL must continuously identify tools that can enhance and support ICE's law enforcement and intelligence mission.

4. OBJECTIVE

ShadowDragon SocialNet access is provided through the Maltego application. The platform can be installed on NON-IRMNET laptops currently deployed across the HSI enterprise. This requirement is to allow HSI-Intel access to ShadowDragon SocialNet.

ShadowDragon develops cyber intelligence solutions that provide threat-related information to organizations, enabling them to stop and attribute targeted actions of malicious actors in the physical or digital world. These solutions are achieved through monitoring and analyzing data from proprietary threat databases, the Internet and the dark web. ShadowDragon is used to by hundreds of private businesses, intelligence and law enforcement organizations globally.

ShadowDragon, will allow HSI-INTEL access to the tools, identified below, in support of its investigative mission(s):

SocialNet is a unique interactive data mining tool that renders directed graphs for link analysis. The results are visualized in minutes to reveal detailed 1 to 1 correlation as well as larger networks of associates. Features include:

5. SPECIFIC REQUIREMENTS/TASKS

The Government requirements are:

The Government requires a database with the capacity to analyze large amounts of multi-lingual data from disparate sources in near real time by leveraging publicly available information through a geo-enabled, text analytics, social media, and web-monitoring platform.

The Government requires a database with the ability to glean information from multiple sources, including, but not limited to:

- Easy, fast, and reliable visualization of people's profile information and relationships
- Search 60+ social networking sites and other account based online entities.
- Complete multiple queries in minutes, which would take hours or days to complete manually.
- Visualize 1 to 1 correlations as well as multiple relationships and networks of people into the 1000s of records.
- Reliable and accurate results with a proprietary data collection/query methodology that has been refined over five years and is continually updated.

6. OTHER APPLICABLE CONDITIONS

6.1. Period of Performance

The period of performance for this contract is a one (1) twelve (12) month base year.

6.2. Place of Performance

ICE Immigration and Customs Enforcement Homeland Security Investigations US Footprint.

7. SECTION 508 COMPLIANCE

Section 508 Requirements

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

Section 508 Requirements for Technology Products

Section 508 applicability to Information and Communications Technology (ICT): SocialNet w/Maltigo

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components (including but not limited to Internet or Intranet website): Does not apply

Applicable 508 requirements for software features and components (including but not limited to Software infrastructure): All requirements in Chapter 5 apply, including all WCAG 2.0 Level A and AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

Applicable 508 requirements for hardware features and components: Does not apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Section 508 Deliverables

Section 508 Accessibility Conformance Reports: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

8. GOVERNMENT ACCEPTANCE PERIOD

The COR/technical representative will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR/technical representative will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

The COR/technical representative will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

The COR will have 5 business days to review deliverables and make comments. The Contractor shall have 10 business days to make corrections and redeliver.

All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Program Management Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

9. DELIVERABLES

All deliverables shall be prepared as subscription services licenses.

10. GENERAL CYBERSECURITY CONTRACTS REQUIREMENT

IMPORTANT CAUTION
Reference to contract requirements and clauses is current as of the date of publication. Due diligence should be exercised by all stakeholders in the process to confirm accuracy and applicability of the requirements identified in this Appendix.

In accordance with ITAR 4.5.4.1 – Compliance with DHS Security Policy Terms and Conditions.
The following requirement should be incorporated into all acquisition documents for ***CLASSIFIED REQUESTS****:*
Compliance with DHS Security Policy Terms and Conditions:
All hardware, software, and services provided under this task order must be compliant with *DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018' for NSS Collateral (Unclass, Secret or Top Secret Collateral).*
In accordance with ITAR 4.5.3.1 – Compliance with DHS Security Policy Terms and Conditions.
The following requirement should be incorporated into all acquisition documents for ***SBU REQUESTS****:*
Compliance with DHS Security Policy Terms and Conditions:
All hardware, software, and services provided under this task order must be compliant with *DHS 4300A DHS Sensitive System Policy* and *DHS 4300A Sensitive Systems Handbook.*
In accordance with ITAR 4.5.3.4 and ITAR 4.5.4.4 – Security Review
The following clause should be incorporated into ***ALL*** *acquisition documents:*
Security Review Terms and Conditions
The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. Access shall be provided to the extent necessary 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 ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.
In accordance with ITAR 4.5.3.7 – Supply Chain Risk Management
The following clause should be incorporated into ***ALL*** *acquisition documents, but exclude services-only contracts:*
Supply Chain Risk Management Terms and Conditions
The Contractors supplying the Government hardware and software shall provide the manufacturer's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNs number of those suppliers must also be provided. Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.
The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.
Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses

internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.

The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

The Supply Chain Risk Management Plan shall address the following elements:

(i) How risks from the supply chain will be identified;

(ii) What processes and security measures will be adopted to manage these risks to the system or system components; and

How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Representative (COR/CO) 30 days post award.

The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents a risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standard certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the CO. Contractors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

The Contractor shall be excused from using new OEM (i.e. "grey market, "previously used) components only with formal Government approval. Such components shall be procured from their original source and have them shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e., until the “end of life"). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

The Contractor is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

In accordance with HSAR 3052.204-70 - Security requirements for unclassified IT resources, with ITAR 4.5.3.3 – Access to Unclassified Facilities, IT Resources, and Sensitive Information Requirement Clause Inclusion Instruction, with ITAR 4.5.3.9 – Security Requirements for Unclassified Information Technology Resources Clause, with ITAR 4.5.4.6 – Required Protections for DHS Systems Hosted in Non-DHS Data Centers, and with ITAR 4.5.4.7 – Contractor Employee Access Clause . As prescribed in

(HSAR) 48 CFR 3004.470-3 **Contract clauses:**

*The following clause should be incorporated into **ALL** acquisition documents:*

Security Requirements For Unclassified Information Technology Resources (JUN 2006)

The Contractor shall be responsible for IT security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

Within [*insert number of days*] days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer (CO), shall be incorporated into the contract as a compliance document.

The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the FISMA of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

Examples of tasks that require security provisions include:

a) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
b) Access to DHS networks or computers at a level beyond that granted the public (e.g., such as bypassing a firewall).

At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

A.5.1 Contractor IT Security Accreditation

The following clause should only be incorporated into acquisition documents involving contractor systems that house ICE data:

Contractor IT Security Accreditation

Within 6 months after contract, the contractor shall submit written proof of IT Security accreditation to DHS for approval by DHS CO. Accreditation will proceed according to the criteria of DHS Sensitive System Policy Publication, 4300A (most current version) or any replacement publication, which the CO will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the CO, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

A.6In accordance with HSAR 3052.204-71 - Contractor Employee Access

*The following clause should be incorporated into **ALL** acquisition documents:*

Contractor Employee Access (Sep 2012)

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:

a) 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);
b) 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);
c) 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
d) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
e) "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.

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 CO. Upon the CO'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.

The CO 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.

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 CO. 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.

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.

A.7In accordance with ITAR 4.5.3.10 – Contractor Employee Access Clause (use language from HSAR 3052.204-70 and alternates at 3052.204-71).

[OCIO IAD Internal Notes

If the contractor requires recurring access to government facilities, or will require access to sensitive information, as prescribed in (HSAR) 48 CFR 3004.470-3(b), insert a clause substantially the same as HSAR 3052.204-70 (extracted above), with appropriate alternates located in HSAR 3052.204-71.

The chart describes how to apply HSAR 3052.204-71 to acquisition documents:

Task requires recurring access to Government facilities or access to sensitive information

- *Basic Clause (HSAR 3052.204-70)*

Requires access to IT resources

- *Basic Clause + Alternate I*

No IT access, but access to sensitive information is limited to U.S. Citizens and lawful permanent residents

- *Basic Clause + Alternate II*

End of OCIO IAD Internal Notes]

*The following Alternate clauses should be evaluated for **ALL** acquisition documents:*

A.7.1 Alternate I

When the contract will require Contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

Contractor IT Resource Access (Sep 2012)

1) 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.
2) 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.
3) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).
4) 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.
5) 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:
    a) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
    b) The waiver must be in the best interest of the Government.
6) 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.

A.7.2 Alternate II

When the Department has determined the contract will not require access to IT resources, but contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, add the following paragraphs:

Sensitive Information Limited to U.S. Citizens and Lawful Permanent Residents (JUN 2006)

1) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.
2) 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

A.8In accordance with White House Digital Government BYODTK – Privacy Expectations

*The following passage should be included in **ALL** acquisition documents:*

Privacy Expectations

Government contractor employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at any time, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed -through that device.

A.9In accordance with White House Digital Government BYODTK – Mobile Information Technology Device Policy

*The following passage should be included in **ALL** acquisition documents for Mobile devices:*

Mobile Information Technology Device Usage

Users who conduct official DHS ICE business on a mobile IT device must:

a) Sign the Remote Access and Mobile IT Device User Agreement Form.
b) Operate the device in compliance with this policy, all applicable federal requirements, and the DHS ICE Remote Access and Mobile Information Technology Guide.
c) Not process or access Classified information on the device.
d) Use only approved and authorized DHS ICE owned devices to physically attach to DHS ICE IT systems.
e) Store only the minimum amount, if any, of Personally Identifiable Information (PII) and electronic Protected Health Information (ePHI) necessary to do one's work, and immediately delete the PII or ePHI when no longer needed. Users shall receive written approval from their supervisor before accessing, processing, transmitting, or storing DHS ICE Sensitive Information such as PII or ePHI.
f) Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.
g) Immediately contact the DHS ICE Service Desk and their immediate supervisor if the IT device is lost, stolen, damaged, destroyed, compromised, or non-functional.
h) Abide by all federal and local laws for using the device while operating a motor vehicle (e.g. users are banned from text messaging while driving federally owned vehicles, and text messaging to conduct DHS ICE business while driving non-government vehicles).

Users who are issued a DHS ICE owned mobile IT device must also:

a. Comply with DHS 4300A Sensitive Systems Handbook Attachment Q.
b. Not disable or alter security features on the device.
c. Only use the DHS ICE owned device for official government use and limited personal use.
d. Reimburse the OCIO for any personal charges incurred that are above the established fixed cost for the Agency's use of the device (e.g. roaming charges incurred for personal calls).
e. Be required to reimburse DHS ICE if the mobile IT device is lost, stolen, damaged or destroyed as a result of negligence, improper use, or willful action on the employee's part and if determined by ICE.

A.10 In accordance with HSAR Class Deviation 15-01, Special Clause, Safeguarding of Sensitive Information (MAR 2015)

*The following clause should be incorporated into acquisition documents for **High Risk Contracts, defined as contracts that consist of contractors or sub-contractors viewing ICE sensitive data, contracts that are performed off-site, and/or contracts that are performed out of the continental United States**:*

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* (most current version), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (most current version), 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.*

A.11 In accordance with HSAR Class Deviation 15-01, Special Clause, Information Technology Security and Privacy Training (MAR 2015)

The following clauses should be incorporated into acquisition documents for ***High Risk Contracts, defined as contracts that consist of contractors or sub-contractors viewing ICE sensitive data, contracts that are performed off-site, or contracts that are performed out of the continental United States****:*

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.

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.

11. SECURITY REQUIREMENTS

GENERAL

Performance under this agreement will require access to Classified National Security Information (NSI) by contractor employees. Contract agreement # XXXXXXXX requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) may access Classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the *National Industrial Security Program Operating Manual (NISPOM)* for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor has access to classified information at an ICE or other Government Facility, it will abide by the requirements set by the agency.

In conjunction with acquisition XXXXXXXX the contractor shall ensure all investigative, reinvestigate, and adjudicative requirements are met in accordance with *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 2-1.

No person shall be allowed to begin work on contract XXXXXXXX and/or access sensitive information related to the contract without ICE receiving clearance verification from the Facility Security Officer (FSO). ICE further retains the right to deem a contractor employee ineligible due to an insufficient background investigation or when derogatory information is received and evaluated under a Continuous Evaluation Program. Any action taken by ICE does not relieve the Contractor from required reporting of derogatory information as outlined under the NISPOM.

The FSO will submit a Visit Authorization Letter (VAL) through the Contracting Officer's Representative (COR) to (b)(7)(E) @ice.dhs.gov for processing contractor employees onto the contract. The clearance verification process will be provided to the COR during Post-Award conference. Note: *Interim TS is not accepted by DHS for access to Top Secret information. The contract employee will only have access to SECRET level information until DoD CAF has granted a final TS.*

See BACKGROUND INVESTIGATIONS paragraph below for processing of contractor employees who will not require access to Classified NSI in support of this agreement.

PRELIMINARY FITNESS DETERMINATION

ICE will exercise full control over granting, denying, withholding, or terminating unescorted government facility and/or sensitive Government information access for contractor employees, based upon the results of a Fitness screening process. ICE may, as it deems appropriate, authorize, and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary Fitness determination or final Fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable preliminary Fitness determination or final Fitness determination by OPR-PSU. Contract employees are

processed under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), or successor thereto; those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the Fitness screening process. (Sexual Abuse and Assault Prevention Standards) implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003)

BACKGROUND INVESTIGATIONS (Process for personnel not requiring access to classified information):

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the Personnel Security Unit. Contractor employees nominated by a Contracting Officer Representative for consideration to support this contract shall submit the following security vetting documentation to OPR-PSU, through the Contracting Officer Representative (COR), within 10 days of notification by OPR-PSU of nomination by the COR and initiation of an Electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

1. Standard Form 85P (Standard Form 85PS (With supplement to 85P required for armed positions)), "Questionnaire for Public Trust Positions" Form completed on-line and archived by the contractor employee in their OPM e-QIP account.

2. Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable – instructions provided to applicant by OPR-PSU). Completed on-line and archived by the contractor employee in their OPM e-QIP account.

3. Two (2) SF 87 (Rev. December 2017) Fingerprint Cards. **(Two Original Cards sent via COR to OPR-PSU)**

4. Foreign National Relatives or Associates Statement. (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

6. Optional Form 306 Declaration for Federal Employment (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

7. If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards) (This document sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

8. One additional document may be applicable if contractor employee was born abroad. If applicable, additional form and instructions will be provided to contractor employee. (If applicable, the document will be sent as an attachment in an e-mail to contractor employee from OPR-PSU – must be signed and archived into contractor employee's OPM e-QIP account prior to electronic "Release" of data via on-line account)

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under reciprocity. The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

An adequate and current investigation is one where the investigation is not more than five years old, meets the contract risk level requirement, and applicant has not had a break in service of more than two years. (Executive Order 13488 amended under Executive Order 13764/DHS Instruction 121-01-007-01)

Required information for submission of security packet will be provided by OPR-PSU at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU as notified by the COR.

To ensure adequate background investigative coverage, contractor employees must currently reside in the United States or its Territories. Additionally, contractor employees are required to have resided within the Unites States or its Territories for three or more years out of the last five (ICE retains the right to deem a contractor employee ineligible due to insufficient background coverage). This timeline is assessed based on the signature date of the standard form questionnaire submitted for the applied position. Contractor employees falling under the following situations may be exempt from the residency requirement: 1) work or worked for the U.S. Government in foreign countries in federal civilian or military capacities; 2) were or are dependents accompanying a federal civilian or a military employee serving in foreign countries so long as they were or are authorized by the U.S. Government to accompany their federal civilian or military sponsor in the foreign location; 3) worked as a contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation; 4) studied abroad at a U.S. affiliated college or university; or 5) have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a federal or contractor employee position, barring any break in federal employment or federal sponsorship.

Only U.S. Citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007-001. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted as outlined under DHS Instruction 121-01-007-001.

TRANSFERS FROM OTHER DHS CONTRACTS (Unclassified support position):

Contractor employees may be eligible for transfer from other DHS Component contracts provided they have an adequate and current investigation meeting the new assignment requirement. If the contractor employee does not meet the new assignment requirement a DHS 11000-25 with ICE supplemental page will be submitted to OPR-PSU to initiate a new investigation.

Transfers will be accomplished by submitting a DHS 11000-25 with ICE supplemental page indicating "Contract Change." The questionnaire related to 6 CFR § 115.117 listed above in item 7 will be required for positions designated under PREA.

CONTINUED ELIGIBILITY

ICE reserves the right and prerogative to deny and/or restrict facility and information access of any contractor employee whose actions conflict with Fitness standards contained in DHS Instruction 121-01-007-01, Chapter 3, paragraph 6.B or who violate standards of conduct under 6 CFR § 115.117. The Contracting Officer or their representative can determine if a risk of compromising sensitive Government information exists or if the efficiency of service is at risk and may direct immediate removal of a contractor employee from contract support. The OPR-PSU will conduct periodic reinvestigations every 5 years, or when derogatory information is received, to evaluate continued Fitness of contractor employees.

REQUIRED REPORTING:

The Contractor will notify OPR-PSU, via the COR, of all terminations/resignations of contractor employees under the contract within five days of occurrence. The Contractor will return any expired ICE issued identification cards and building passes of terminated/ resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contractor employees under the contract to the OPR-PSU, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the contractor employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR a Quarterly Report containing the names of contractor employees who are active, pending hire, have departed within the quarter, or have had a legal name change (Submitted with documentation). The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

CORs will submit reports to (b)(7)(E) @ice.dhs.gov

Contractors, who are involved with management and/or use of information/data deemed "sensitive" to include 'law enforcement sensitive" are required to complete the DHS Form 11000-6-Sensitive but Unclassified Information NDA for contractor access to sensitive information. The NDA will be administered by the COR to the all-contract personnel within 10 calendar days of the entry on duty date. The completed form shall remain on file with the COR for purpose of administration and inspection.

Sensitive information as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, *DHS Policy for Sensitive Information* and ICE Policy 4003, *Safeguarding Law Enforcement Sensitive Information*."

Any unauthorized disclosure of information should be reported to (b)(7)(E) @ICE.dhs.gov.

The contractor is required to report certain events that have an impact on the status of the facility clearance (FCL) and/or the status of a contractor employee's personnel security clearance as outlined by *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter1-3, Reporting Requirements. Contractors shall establish internal procedures as are necessary to ensure that cleared personnel are aware of their responsibilities for reporting pertinent information to the FSO and other federal authorities as required.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU 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 the OPR-PSU 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.

Contractors shall provide all employees supporting contract XXXXXXXX proper initial and annual refresher security training and briefings commensurate with their clearance level, to include security awareness, defensive security briefings. (*National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 3-1. The contractor shall forward a roster of the completed training to the COR on a quarterly basis.

INFORMATION TECHNOLOGY SECURITY CLEARANCE

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS MD 4300.1*, Information Technology Systems Security.* or its replacement. Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.
Contractor employees who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

In accordance with Chief Information Office requirements and provisions, all contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Information Assurance Awareness Training (IAAT) will be required upon initial access and annually thereafter. IAAT training will be provided by the appropriate component agency of DHS.

Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on PALMS or by contacting ICE.ADSEC@ICE.dhs.gov. Department contractor employees, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. System Administrators should be aware of any unusual or inappropriate behavior by personnel

accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

DHS ENTERPRISE ARCHITECTURE COMPLIANCE

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA, NIST & FISMA requirements:

• All developed solutions and requirements shall be compliant with the HLS EA.
• All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
• 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.
• 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.
• 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 8 ITAR Quick Essentials Guide 2011 v2.0 Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.
• Integrate federal cyber security requirements to include, but not limited to the DHS 4300A Sensitive System Policy, applicable National Institute of Technology (NIST) 800 series documentation, and the Federal Information Security Management Act (FISMA) of 2014 into technical solutions and provide strategies to meet on-going operational security controls in areas such as security patching, configuration management, authentication, and security monitoring.

IT 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)

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)

From: (b)(6); (b)(7)(C)
Sent: Mon, 23 Mar 2020 18:50:07 +0000
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: System Trial Question
Attachments: SOW_ShadowDragon 6MAR20.doc

I've attached the draft ShadowDragon Statement of Work as a template to submit to Privacy for use approval, linked below. I haven't shot this to the CIOs yet because full edits have not come back from OPLA and Privacy, but it'll get you on the right track.

(b)(7)(E)

Best,
(b)(6);

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Sent: Monday, March 23, 2020 12:36 PM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: System Trial Question

(b)(6);

Good afternoon. How are you? I hope that you are safe and healthy during this crazy time.

As we discussed at the CIO session earlier this month, HSI Newark was recently provided with a demonstration of the system detailed below and attached. The vendor is reaching out to set-up a free trial, but as you brought to my attention this needs to be cleared through Privacy. Do you have any information/insight/templates that you can provide me regarding this process? Is there any information that I should elicit from the vendor that Privacy may need in order to start this process? Are there any specific questions that I should ask the vendor? I've copied SIP-NJ Group Supervisor (b)(6); (b)(7)(C) for visibility as she will be participating in establishing the system trial with the vendor.

This seemed like a really good tool and I would like to have the system trial if possible. However, I obviously want to go about it the right way. Would you please let me know at your first opportunity as the vendor would like to set-up a call this week.

Please contact me if you have any questions or concerns. Thank you.

(b)(6);

(b)(6); (b)(7)(C)
Chief Intelligence Officer
U.S. Immigration and Customs Enforcement

HSI Newark
Office: 973-954 (b)(6); (b)(7)(C)
Mobile: 973-391

From: (b)(6); (b)(7)(C)
Sent: Monday, March 23, 2020 11:56 AM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: (b)(7)(E)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C); (b)(7)(E)

Regards,
(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) Business Development / Sales Director

Office: +1 212-201 (b)(6); **Cell:** +1 860-462 (b)(6);
Fax (b)(7)(E) **Website** (b)(7)(E)

(b)(7)(E)