U.S. Department of Justice
Drug Enforcement Administration
FOI/Records Management Section
8701 Morrissette Drive
Springfield, Virginia 22152

JUN 0 8 2017

Case Number: 17-00602-F

Subject: DEA Contract with Verint Technology Incorporated (DJD13C0016)

Joseph Cox
MuckRock
DEPT MR 37898
411A Highland Ave
Somerville, MA 02144-2516

Dear Mr. Cox:

This letter responds to your Freedom of Information/Privacy Act (FOI/PA) request dated May 22, 2017, addressed to the Drug Enforcement Administration (DEA), Freedom of Information/Privacy Act Unit (SARF), seeking access to information regarding the above subject.

The processing of your request identified certain materials that will be released to you. Portions not released are being withheld pursuant to the Freedom of Information Act, 5 U.S.C. § 552, and/or the Privacy Act, 5 U.S.C. § 552a. Please refer to the list enclosed with this letter that identifies the authority for withholding the deleted material, which is indicated by a mark appearing in the block next to the exemption. An additional enclosure with this letter explains these exemptions in more detail. The documents are being forwarded to you with this letter.

The rules and regulations of the Drug Enforcement Administration applicable to Freedom of Information Act requests are contained in the Code of Federal Regulations, Title 28, Part 16, as amended. They are published in the Federal Register and are available for inspection by members of the public.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. *See* 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may contact our FOIA Public Liaison at 202-307-7596 for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, DC 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: https://foiaonline.regulations.gov/foia/action/public/home. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

If you have any questions regarding this letter, you may contact Government Information Specialist Stephanie L. Evans at 202-307-7733.

Sincerely,

Katherine Myrick

Katherine L. Myrick, Chief
Freedom of Information/Privacy Act Unit
FOI/Records Management Section

Number of pages released: 70

APPLICABLE SECTIONS OF THE FREEDOM OF INFORMATION AND/OR PRIVACY ACT:

Freedom of Information Act 5 U.S.C. 552			**Privacy Act 5 U.S.C. 552a**	
[ ] (b)(1)	[ ] (b)(5)	[ ] (b)(7)(C)	[ ] (d)(5)	[ ] (k)(2)
[ ] (b)(2)	[X] (b)(6)	[ ] (b)(7)(D)	[ ] (j)(2)	[ ] (k)(5)
[ ] (b)(3)	[ ] (b)(7)(A)	[ ] (b)(7)(E)	[ ] (k)(1)	[ ] (k)(6)
[X] (b)(4)	[ ] (b)(7)(B)	[ ] (b)(7)(F)		

Enclosure(s)

EXPLANATION OF EXEMPTIONS
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
(b)(2) related solely to the internal personnel rules and practices of an agency;
(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), if that statute-
(A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and (B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.
(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;
(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
(k)(4) required by statute to be maintained and used solely as statistical records;
(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24 & 30

1. REQUISITION NUMBER	OMB Clearance Control Number
PR D-13-OS-0086	1103-0018

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
DJD-13-C-0016	see box 31c		QS DJD-13-R-0007	12/07/2012

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE / LOCAL TIME
	Rebecca Stegall		12/13/2012 14:00:00

9. ISSUED BY	CODE	HQ
DEA Headquarters 8701 Morrissette Drive, Attn: (FACI/REBECCA STEGALL) Springfield, VA 22152		

10. THIS ACQUISITION IS: ☐ UNRESTRICTED OR ☒ SET ASIDE: 0 % FOR:
☐ SMALL BUSINESS ☐ WOMAN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS
NAICS: 541519
☐ HUBZONE SMALL BUSINESS ☐ ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)
SIZE STANDARD: 007
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ 8(A)

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING	14. METHOD OF SOLICITATION
☐ SEE SCHEDULE	NET 30	☐		☐ RFQ ☐ IFB ☒ RFP

15. DELIVER TO	CODE	SOD
DEA - Special Operations Division 14560 Avion Parkway, Attn: (b)(6) Chantilly, VA 20151		

16. ADMINISTERED BY	CODE	HQ
DEA Headquarters 8701 Morrissette Drive, Attn: (FACI/REBECCA STEGALL) Springfield, VA 22152		

17a. CONTRACTOR/ OFFEROR	CODE	541924753	FACILITY CODE	100549828
VERINT TECHNOLOGY INC 330 SOUTH SERVICE ROAD MELVILLE, NY 11747-3257				

TELEPHONE NO.

17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER ☐

18a. PAYMENT WILL BE MADE BY	CODE	SOD
DEA - Special Operations Division 14560 Avion Parkway, Attn: (invoice.speops@usdoj.gov) Chantilly, VA 20151		

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
0001	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN To be performed in accordance with the attached SOW See Continuation Sheet(s)	(b)(4)			

25. ACCOUNTING AND APPROPRIATION DATA
2013-2013-S1R-OS-2560000-DOM-G2-01LK-ENF-25218-SOD-2560000

26. TOTAL AWARD AMOUNT (For Govt. Use Only)
$1,447,294.80

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED
☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☒ ARE NOT ATTACHED

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

☐ 29. AWARD OF CONTRACT: REF. OFFER DATED. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)
	Lisa Taylor

30b. NAME AND TITLE OF SIGNER (Type or print)	30c. DATE SIGNED	31b. NAME OF THE CONTRACTING OFFICER (Type or print)	31c. DATE SIGNED
Alfredo Barresi - President	12/19/2012	Taylor,Lisa	12-20-12

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 6/2011)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER
38. S/R ACCOUNT NO.	39. S/R VOUCHER NUMBER	40. PAID BY		

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

STANDARD FORM 1449 (REV. 5/2011) **BACK**

Section 2 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
	Line Period of Performance: 01/01/2013 - 12/31/2013	(b)(4)			
0002	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN				
	Line Period of Performance: 01/01/2014 - 12/31/2014				
0003	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN				
	Line Period of Performance: 01/01/2015 - 12/31/2015				
0004	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN				
	Line Period of Performance: 01/01/2016 - 12/31/2016				
0005	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN				
	Line Period of Performance: 01/01/2017 - 12/31/2017				
				TOTAL	$1,447,294.80

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	[redacted]	[redacted]
N/A	1	(b)(4)	2013 - S1R - OS - 2560000 - DOM-G2 - 01LK - ENF - 25218 - - - SOD - - - 2560000

Section 3 – Contract Clauses

3.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: www.aquisition.gov/far.

(End of clause)

52.202-1	Definitions	JAN 2012
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	APR 1984
52.203-6	Restrictions On Subcontractor Sales To The Government	SEP 2006
52.203-7	Anti-Kickback Procedures	OCT 2010
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	JAN 1997
52.203-10	Price Or Fee Adjustment For Illegal Or Improper Activity	JAN 1997
52.203-11	Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions.	SEP 2007
52.203-12	Limitation On Payments To Influence Certain Federal Transactions	OCT 2010
52.204-4	Printed or Copied Double-Sided on Post-Consumer Fiber Content Paper	MAY 2011
52.204-7	Central Contractor Registration	AUG 2012
52.204-13	Central Contractor Registration Maintenance	DEC 2012
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	AUG 2012
52.209-6	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment	DEC 2010
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	FEB 2012
52.222-3	Convict Labor	JUN 2003
52.222-21	Prohibition of Segregated Facilities	FEB 1999
52.222-26	Equal Opportunity	MAR 2007
52.222-35	Equal Opportunity for Veterans	SEP 2010
52.222-36	Affirmative Action for Workers with Disabilities	OCT 2010
52.222-37	Employment Reports Veterans	SEP 2010
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	DEC 2010
52.222-50	Combating Trafficking in Persons	FEB 2009

52.223-6	Drug-Free Workplace	MAY 2001
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving	AUG 2011
52.225-13	Restrictions on Certain Foreign Purchase	JUNE 2008
52.225-25	Prohibition on contracting with Entities Engaging in Sanctioned Activities Relating to Iran – Representation and Certification	DEC 2012
52.227-1	Authorization and Consent	DEC 2007
52.229-3	Federal, State, and Local Taxes	APR 2003
52.232-1	Payments	APR 1984
52.232-8	Discounts for Prompt Payment	FEB 2002
52.232-9	Limitation on Withholding of Payments	APR 1984
52.232-17	Interest	OCT 2010
52.232-18	Availability Of Funds	APR 1984
52.232-23	Assignment Of Claims	JAN 1986
52.232-25	Prompt Payment	OCT 2008
52.232-33	Payment by Electronic Funds Transfer -Central Contractor Registration	OCT 2003
52.233-1	Disputes	JUL 2002
52.233-3	Protest After Award	AUG 1996
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004
52.237-3	Continuity Of Services	JAN 1991
52.242-13	Bankruptcy	JUL 1995
52.243-1	Changes – Fixed Price	AUG 1987
52.244-6	Subcontracts for Commercial Items	DEC 2010
52.246-4	Inspection of Services – Fixed Price	AUG 1996
52.246-25	Limitation Of Liability--Services	FEB 1997
52.249-4	Termination For Convenience Of The Government (Services)(Short Form)	APR 1984
52.249-8	Default (Fixed-Price Supply and Service)	APR 1984
52.253-1	Computer Generated Forms	JAN 1991

CLAUSES INCORPORATED BY FULL TEXT

3.2 DEA-2852.247-70 GENERAL PACKAGING AND MARKING REQUIREMENTS (MAY 2012)

Packaging and packing for all items (includes written materials, reports, presentations, etc.) delivered hereunder shall be in accordance with common commercial practices, adequate to insure protection from possible damage resulting from improper handling, inclement weather, water damage, excessive heat and cold, and to insure acceptance by a common carrier for safe delivery to its final destination.

All deliverables shall clearly indicate the purchase order number, BPA number and call number, or contract number and/or task (delivery) order number, whichever is appropriate, on or adjacent to the exterior shipping label.

(End of clause)

3.4 DEA-2852.211-70 PERIOD OF PERFORMANCE (BASE AND OPTIONS) (MAY 2012)

(a) The period of performance of Base Period of this contract begins on January 1, 2013 and ends on December 31, 2013.

(b) Pursuant to clause 52.217-9, Option to Extend the Term of the Contract, in the event that the Contracting Officer exercises an option, the period of performance for each option period shall be as follows:

Option Period I: January 1, 2014 through December 31, 2014
Option Period II: January 1, 2015 through December 31, 2015
Option Period III: January 1, 2016 through December 31, 2016
Option Period IV: January 1, 2017 through December 31, 2017

(c) The exercise of any options is subject to the availability of funding and the continuing needs of the Government.

(End of clause)

3.5 DEA-2852.242-73 CONTRACTING OFFICER'S REPRESENTATIVE (MAY 2012)

Pursuant to FAR 1.602-2, the following individual has been designated as the Contracting Officer's Representative (COR) under this contract:

Tracey Brooks/Tracey.E.Brooks@usdoj.gov/703-488-4400

(b) The COR has responsibility for performing contract administration, which includes, but is not limited to, the following duties: functioning as the technical liaison with the contractor; monitoring the contractor's performance and progress of the work; receiving, inspecting, and accepting all deliverables or services provided under the contract; and reviewing all invoices/vouchers submitted for payment.

(c) The COR does not have the authority to alter the contractor's obligations under the contract, and/or modify any of the expressed terms, conditions, specifications, or cost of the agreement. If as a result of technical discussions it is desirable to alter/change contractual obligations or the Scope of Work, the Contracting Officer shall issue such changes.

(End of clause)

3.6 TASK MONITOR(S)

(a) The Task Monitor will be designated upon contract award. Joe Moorefield

(b) The Task Monitor is responsible for: receiving all deliverables; inspecting and accepting the supplies or services provided hereunder in accordance with the terms and conditions of this contract; providing direction to the Contractor which clarifies technical aspects of the contract effort, fills in details or otherwise serves to accomplish the contractual scope of work; evaluating performance; certifying acceptance of supplies or services prior to payment, and approving invoices/vouchers.

(c) The Task Monitor does not have the authority to alter the Contractor's obligations under the task order, direct changes and/or modify any of the expressed terms, conditions, specifications, or cost of the contract.

3.7 DEA-2852.242-74 CONTRACT ADMINISTRATION POINTS OF CONTACT (MAY 2012)

(a) The Contract Administration Office for this contract is:

U. S. Department of Justice
Drug Enforcement Administration
Office of Acquisition and Relocation Management (FA)
8701 Morrissette Drive
Springfield, VA 22152

Contract Specialist/telephone #/email: Rebecca Stegall, 202-307-1323, Rebecca.V.Stegall@usdoj.gov

Contracting Officer/telephone #/email: Lisa Taylor, 202-307-7820, Lisa.Taylor2@usdoj.gov

Contracting Officer's Representative (COR): See 3.5.

(b) Contract administration for the contractor shall be performed by:

Name: Al Barresi./al.barresi@verint.com

(End of clause)

3.8 DEA-2852.242-71 INVOICE REQUIREMENTS (MAY 2012)

(a) The Contractor shall submit scanned or electronic images of invoice(s) to the following e-mail addresses:

(1) Invoice.specops@usdoj.gov;
(2) Contract Specialist: Rebecca.V.Stegall@usdoj.gov; and
(3) Contracting Officer's Representative: Tracey.E.Brooks@usdoj.gov

(b) The date of record for invoice receipt is established on the day of receipt of the e-mail if it arrives before the end of standard business hours (5 p.m. local), or the next business day if the invoice arrives outside of normal business hours. Scanned documents with original signatures in .pdf or other graphic formats attached to the e-mail are acceptable. Digital/electronic signatures and certificates cannot be processed by DEA and will be returned.

(c) In addition to the items specified in FAR 32.905(b), a proper invoice shall also include the following minimum additional information and/or attached documentation:

(1) Total/cumulative charges for the billing period for each Contract Line Item Number (CLIN);
(2) Dates upon which items/services were delivered; and
(3) The Contractor's Taxpayer Identification Number (TIN).

(d) Invoices will be rejected if they are illegible or otherwise unreadable, or if they do not contain the required information or signatures.

(End of clause)

3.9 DEA-2852.242-72 FINAL INVOICE AND RELEASE OF RESIDUAL FUNDS (MAY 2012)

The Contractor shall submit a copy of the final invoice to the Contracting Officer at the address listed in clause DEA-2852.242-71, Invoice Requirements. The final invoice must be marked "Informational Copy – Final Invoice."

By submission of the final invoice and upon receipt of final payment, the Contractor releases the Government from any and all claims arising under, or by virtue of, this contract. Accordingly,

the Government shall not be liable for the payment of any future invoices that may be submitted under the above referenced order.

If residual funds on the contract total $100 or less after payment of the final invoice, the Government will automatically deobligate the residual funds without further communication with the vendor.

If funds greater than $100 remain on this order after payment of the final invoice, the Government will issue a bilateral modification to deobligate the residual funds. The contractor will have up to 30 calendar days after issuance of the modification to sign and return it. The contractor's signature on the modification shall constitute a release of all claims against the Government arising by virtue of this contract, other than claims, in stated amounts, that the Contractor has specifically exempted from the operation of the release. If the contractor fails to sign the modification or assert a claim within the stated period, the Government will deobligate the residual balance and proceed with close-out of the contract.

(End of clause)

3.10 DEA-2852.204.85 SECURITY REQUIREMENTS FOR ACCESS TO SECRET INFORMATION DOD/DSS (MAY 2011)

DEA's personnel, information, and facility security requirements for contracts, task orders, delivery orders, purchase orders, blanket purchase agreements, reimbursable agreements, and other type of contractual agreements (hereafter referred to as "contract" and "Contractor") to provide goods and services to DEA are hereby provided for the subject access level. This clause is available on-line at www.dea.gov; click on Doing Business with DEA; scroll to DEA Security Provisions; and click on DEA-2852.204.85.

3.11 DEA-2852.209-70 ORGANIZATIONAL CONFLICTS OF INTEREST (MAY 2012)

The Contractor warrants that, to the best of its knowledge and belief, there are no relevant facts or circumstances that would give rise to an organizational conflict of interest as described in FAR Subpart 9.5, or that the Contractor has disclosed all such relevant information.

In the event that an actual, potential, or apparent organizational conflict of interest is discovered after award, the Contractor shall make full disclosure of the particular facts and circumstances to the Contracting Officer in writing. This disclosure shall include a description of the actions that the Contractor has taken, or proposes to take in order to avoid, mitigate, or neutralize the risk to the Government.

Remedies. The Contracting Officer may terminate this contract for convenience, in whole or in part, if deemed necessary to avoid or mitigate an actual or apparent organizational conflict of interest. In the event that the Contractor failed to disclose in a timely manner, or misrepresented the facts and circumstances of, an actual, potential, or apparent organizational conflict of interest of

which it had prior knowledge, the Contracting Officer may terminate this contract for default or cause, and pursue additional remedies, including debarment, as may be provided by law.

The Contractor shall insert terms substantially similar to this clause in any subcontract or consultant agreement under this contract.

(End of clause)

3.12 DEA-2852.209-73 REPRESENTATION REGARDING FELONY CONVICTION UNDER ANY FEDERAL LAW OR UNPAID DELINQUENT TAX LIABILITY (DEVIATION 2012-02) (MAY 2012)

(a) In accordance with sections 543 and 544 of Title V, Division B of the Further Continuing Appropriations Act, 2012 (Pub. L. 112-55), none of the funds made available by that Act may be used to enter into a contract, memorandum of understanding, or cooperative agreement with a corporation

(1) Convicted of a felony criminal violation of any Federal law within the preceding 24 months, or

(2) With an unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability,

unless an agency has considered suspension and debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.

(b) ***By accepting this award or order, in writing or by performance***, the offeror/contractor represents that

(1) The offeror/contractor is not a corporation convicted of a felony criminal violation under any Federal law within the preceding 24 months; and

(2) The offeror/contractor is not a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.

(End of clause)

3.13 DEA-2852.218-70 CONTINUING CONTRACT PERFORMANCE DURING A PANDEMIC INFLUENZA OUTBREAK OR OTHER BIOMEDICAL EMERGENCY OR CATASTROPHE (MAY 2012)

(a) It has been determined that the services provided under this contract are mission-critical and essential to the ongoing operations of the Drug Enforcement Administration.

(b) In the event of a pandemic influenza outbreak or other biomedical emergency or catastrophe, the Contractor shall continue performance of this contract without delay or interruption.

(c) The Government will provide notice, information, and instructions to the Contractor regarding any such event. If it is determined that changes to the performance requirements are necessary, the Government will implement the necessary changes by the issuance of Change Orders in accordance with the Changes clause of the contract, and the Contractor may assert its right for an equitable adjustment accordingly.

(d) Additional information and guidance is provided in the notice entitled, "Continuing Contract Performance During a Pandemic Influenza or Other National Emergency," which may be viewed at http://www.justice.gov/dea/acquisitions_contracts.html.

(End of clause)

3.14 DEA-2852.242-78 APPROVAL REQUIRED FOR ADVERTISING AND MEDIA RELEASES (MAY 2012)

The Contractor shall not release, publish, or otherwise disseminate any information regarding this contract or the specifics of the requirement in any public or private media, publication, or venue without the prior written approval of the Contracting Officer. Media communication releases pertaining to any aspect of the award or performance thereunder shall not be made without the prior written approval of the Contracting Officer.

(End of clause)

3.15 DEA-2852.209-71 LIMITATIONS ON FUTURE CONTRACTING (MAY 2012)

(a) Work under this contract may provide the Contractor with access to advance information about future Government procurements. This information is not generally available to other persons or firms. In addition, the work may involve the definition of requirements for, or the preparation of specifications for, various systems, equipment, hardware, and/or software. Without the restrictions specified in paragraph (b) below, the Contractor's objectivity in performing the work may be impaired by its other business activities, the nature of the work to be performed may result in an unfair competitive advantage to the Contractor in future Government procurements, or the Contractor's ability to perform work required under future Government contracts in an objective manner may be impaired by its performance of work under this contract.

(b) In order to prevent a potential bias, unfair competitive advantage, or other potential conflict of interest, the Contractor shall be subject to the following restrictions:

(1) The Contractor may be excluded from competition for, or award of, any Government contracts as to which, in the course of performance of this contract, the Contractor has received advance procurement information before such information has been made generally available to other persons or firms.

(2) The Contractor may be excluded from competition for, or award of, any Government contract for which the Contractor actually assists in the development of the Request for Quotation, Specifications or Statement of Work.

(3) The Contractor may be excluded from competition for, or award of, any Government contract that calls for the evaluation of system requirements, system definitions, or other products developed by the Contractor under this contract.

(4) The Contractor may be excluded from competition for, or award of, any Government contract that calls for the construction or fabrication of any system, equipment, hardware, and/or software for which the Contractor participated in the systems engineering and technical direction for the system, including but not limited to the development of requirements or definitions pursuant to this contract.

(c) This clause shall not exclude the Contractor from performing work under any amendment or modification to this contract or from competing for an award for any future contract for work that is the same or similar to work performed under this contract.

(d) The term "Contractor" as used in this clause includes any person, firm or corporation that has a majority or controlling interest in the Contractor or in any parent corporation thereof, and any person, firm or corporation that has a majority or controlling interest in the Contractor, and those of any corporation in which the Contractor (or any parent or subsidiary corporation thereof) has a majority or controlling interest.

(e) The exclusions contained in paragraph (b)(1) through (b)(4) of this provision shall apply for the duration of this contract and for three (3) years after completion and acceptance of all work performed hereunder. The Government may, at its sole discretion, waive any provisions of this clause if deemed in the best interest of the Government.

(End of clause)

3.16 52.209-9 UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS (FEB 2012)

(a) The Contractor shall update the information in the Federal Awardee Performance and Integrity Information System (FAPIIS) on a semi-annual basis, throughout the life of the

contract, by posting the required information in the Central Contractor Registration database via https://www.acquisition.gov.

(b) As required by section 3010 of the Supplemental Appropriations Act, 2010 (Pub. L. 111-212), all information posted in FAPIIS on or after April 15, 2011, except past performance reviews, will be publicly available. FAPIIS consists of two segments—

(1) The non-public segment, into which Government officials and the Contractor post information, which can only be viewed by—

(i) Government personnel and authorized users performing business on behalf of the Government: or

(ii) The Contractor, when viewing data on itself; and

(2) The publicly-available segment, to which all data in the non-public segment of FAPIIS is automatically transferred after a waiting period of 14 calendar days, except for—

(i) Past performance reviews required by subpart 42.15;

(ii) Information that was entered prior to April 15, 2011; or

(iii) Information that is withdrawn during the 14-calendar-day waiting period by the Government official who posted it in accordance with paragraph (c)(1) of this clause.

(c) The Contractor will receive notification when the Government posts new information to the Contractor's record.

(1) If the Contractor asserts in writing within 7 calendar days, to the Government official who posted the information, that some of the information posted to the non-public segment of FAPIIS is covered by a disclosure exemption under the Freedom of Information Act, the Government official who posted the information must within 7 calendar days remove the posting from FAPIIS and resolve the issue in accordance with agency Freedom of Information procedures, prior to reposting the releasable information. The contractor must cite 52.209-9 and request removal within 7 calendar days of the posting to FAPIIS.

(2) The Contractor will also have an opportunity to post comments regarding information that has been posted by the Government. The comments will be retained as long as the associated information is retained, *i.e.*, for a total period of 6 years. Contractor comments will remain a part of the record unless the Contractor revises them.

(3) As required by section 3010 of Pub. L. 111-212, all information posted in FAPIIS on or after April 15, 2011, except past performance reviews, will be publicly available.

(d) Public requests for system information posted prior to April 15, 2011, will be handled under Freedom of Information Act procedures, including, where appropriate, procedures promulgated under E.O. 12600.

(End of clause)

3.17 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

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

3.18 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

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

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **60** months from date of contract award.

(End of clause)
(End of Section)

Section 4 – List of Attachments

Exhibits and Attachments

1. Statement of Work

(End of Section)

STATEMENT OF WORK

1. BACKGROUND

Drug Enforcement Administration (DEA) currently utilizes a Basic Ordering Agreement (BOA) to provide Technical Support and Maintenance including parts and labor. The requirement covers the original T2S2 System, the Front End/Back End (FEBE) Expansion, the additional System Administrator and Workstation Licenses.

2. SCOPE

DEA requires Technical Support and Maintenance including parts and labor for the system.

3. TASKS/DELIVERY

a. The Contractor shall provide a contact support phone number that can be called 24 hours a day 365 days a year to speak with a technical expert or to leave a message for call back by a technical expert with the required security clearance. Telephonic contact with the Contractor must be with a United States (US) citizen and based in the US.

b. The Contractor shall provide telephonic support during normal business hours. Normal hours are considered Monday through Friday, 9 AM to 6 PM EST with the exception of days that are U.S. Government scheduled holidays. During normal business hours, contact response should be received from the Contractor within two hours of first contact with their telephonic support line. After hours and non-business days, to include holidays, the Contractor must call back within three hours after the first contact with their telephonic support line.

c. The Contractor shall provide technical support with subject matter experts to guide a skilled user to perform basic checks over the phone. If additional support is required the Contractor shall provide an onsite cleared subject matter expert. The Contractor shall provide a subject matter expert onsite to troubleshoot a minor problem within two business days and next day response for a major problem. A minor problem is defined as a system problem not related to call delivery or evidence production. A major problem is defined as any problem related to call delivery, real time processing or evidence production.

d. The Contractor shall repair or replace any defective part at no additional cost to the Government. The Contractor can trade out failed equipment and parts with the exception of any device that holds memory or stores data. Those devices shall not leave the Government's site nor can they be turned in for warranty exchange. A hard drive and memory sticks are examples of devices that cannot be traded and must be replaced if defective.

e. The Contractor shall provide a written summary with a detailed explanation of what system or subsystem will be affected prior to any software or firmware being installed or any option changed in DEA's system. The summary shall provide an explanation of the

risks to include impact of any subsystems and the expected benefit(s) to the Government of the new version of software/firmware or option. The summary shall include the estimated time required to install the software and what measures will be taken to minimize the impact while the installation is taking place. The summary must cover the Contractor's plan to restore or revert the system back to the previous status should the upgrade fail or produce unwanted results. The Contractor shall give the Government the option to perform the install during regular business hours or perform after 1:00 AM and ending before 8:00 AM to reduce operational impact at no additional cost to the Government.

f. The Contractor shall keep a stock of most replaceable items that generally fail to prevent a long lead time for part replacement.

g. The Contractor shall keep a log of complaints filed on the system performance. The log shall track and report the status of these complaints monthly to the Government. The log shall list all complaints that are open, all closed within the last 60 days, and those being researched by the Contractor. The log shall contain the nature of the complaint and when the complaint was reported; what subsystem was affected, and how and when the complaint was resolved. No complaint can be closed until the Government agrees to the closure of the complaint.

4. SECURITY

All parties from the Contractor supporting this contract shall be cleared, US citizens with DEA approved NSI SECRET clearance level or higher. The Contractor shall provide and maintain a facility cage code that can support the ability to have cleared individuals working at a Government site with National Security clearances at a minimum of SECRET.

5. PLACE OF PERFORMANCE

The work will be performed at the Special Operations Division.

6. PERIOD OF PERFORMANCE

A contract will be awarded for a base period of one (1) year plus four (4) one-year option periods.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE: DJD-13-C-0016	DMB Clearance Control Number: 1103-0018

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO	5. PROJECT NO. (If applicable)
0001	see block 16c	PR D-13-OS-0086	

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than item 6)	CODE
HQ	HQ		

DEA Headquarters
8701 Morrissette Drive, Attn: (FACI/REBECCA STEGALL)
Springfield, VA 22152

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, state and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO
VERINT TECHNOLOGY INC 330 SOUTH SERVICE ROAD MELVILLE, NY 11747-3257		9B. DATED (SEE ITEM 11)
	X	10A. MODIFICATION OF CONTRACT/ORDER NO: DJD-13-C-0016
		10B. DATED (SEE ITEM 13): 12/20/2012

CODE 541924733 FACILITY CODE 180549828

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: Mutual Agreement of the Parties
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose for this bilateral modification is to incorporate the signed DD-254 along with DOJ 2620.7 CONTROL AND PROTECTION OF LIMITED OFFICIAL USE INFORMATION and DOJ 2640-2F INFORMATION TECHNOLOGY SECURITY into the contract. SOW Section 4 is updated. There are no other changes to the contract. See attachments I, II, III, and SOW replacement page.
A vertical line in the right margin indicates a change in text.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
ALBINO BARRESI / PRESIDENT	Taylor,Lisa
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED: 1/10/13
	16B. UNITED STATES OF AMERICA (Signature of Contracting Officer)
	16C. DATE SIGNED: 1-14-13

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA FAR (48 CFR) 53.243

Section 2 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN **Line Period of Performance:** 01/01/2013 - 12/31/2013	(b)(4)			
				PREVIOUS TOTAL	$1,447,294.80
				CHANGE	$0.00
				CURRENT TOTAL	$1,447,294.80

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)

1. CLEARANCE AND SAFEGUARDING
a. FACILITY CLEARANCE REQUIRED: SECRET
b. LEVEL OF SAFEGUARDING REQUIRED: NONE

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*
- [X] a. PRIME CONTRACT NUMBER: DJD-13-C-0016
- [ ] b. SUBCONTRACT NUMBER:
- [ ] c. SOLICITATION OR OTHER NUMBER: Due Date (YYMMDD):

3. THIS SPECIFICATION IS: *(X and complete as applicable)*
- [X] a. ORIGINAL *(Complete date in all cases)* — Date (YYMMDD): 130109
- [ ] b. REVISED *(Supersedes all previous specs)* — Revision No.: — Date (YYMMDD):
- [ ] c. FINAL *(Complete item 5 in all cases)* — Date (YYMMDD):

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes complete the following:
Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes complete the following:
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Verint Technology, Inc. 330 South Service Road Melville, NY 11747-3257	3ZDW4	Defense Security Service 1600 Stewart Ave, Suite 205 Westbury, NY 11590

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICES *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Drug Enforcement Administration DEA facilities only		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
The contractor will provide information technology support in secure facilities for the Drug Enforcement Administration of the US Department of Justice and will require access to National Security Information in performance of this contract.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	[ ]	[X]	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	[X]	[ ]
b. RESTRICTED DATA	[ ]	[X]	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	[ ]	[X]
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	[ ]	[X]	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	[ ]	[X]
d. FORMERLY RESTRICTED DATA	[ ]	[X]	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	[ ]	[X]
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY	[ ]	[X]
(1) Sensitive Compartmented Information (SCI)	[ ]	[X]	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	[ ]	[X]
(2) Non-SCI	[X]	[ ]	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	[ ]	[X]
f. SPECIAL ACCESS INFORMATION	[ ]	[X]	h. REQUIRE A COMSEC ACCOUNT	[ ]	[X]
g. NATO INFORMATION	[ ]	[X]	i. HAVE A TEMPEST REQUIREMENT	[ ]	[X]
h. FOREIGN GOVERNMENT INFORMATION	[ ]	[X]	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	[ ]	[X]
i. LIMITED DISSEMINATION INFORMATION	[ ]	[X]	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	[ ]	[X]
j. FOR OFFICIAL USE ONLY INFORMATION	[ ]	[X]	l. OTHER *(Specify)* N/A	[ ]	[X]
k. OTHER *(Specify)* Sensitive but Unclassified Information	[X]	[ ]			

DD FORM 254, DEC 1999 PREVIOUS EDITION IS OBSOLETE

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public release shall be submitted for approval prior to release

☐ Direct ☐ Through *(Specify)*.

PUBLIC RELEASE IS NOT AUTHORIZED

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this effort is identified below. If any difficulty is encountered in applyin g this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the offic al identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any document/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*

The contract is for information technology support in secure buildings. Actual knowledge or, generation, or production of classified information is not required for performance of the contract. Cleared personnel are required to perform this service because access to classified information cannot be precluded by escorting personnel. The contractor will provide cleared personnel adequate for the operational needs of the contract.

See attachment.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. *(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)* ☒ Yes ☐ No

DEA security requirements and the documentation required to obtain approval for access at DEA are provided in Security Provision No. DEA-2852-204-85

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office *(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)* ☐ Yes ☒ No

This is an access elsewhere contract; however; the DSS remains responsible for security requirements with the National Industrial Security Program Operating Manual (NISPOM).

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
(b)(6)	DEPARTMENT SECURITY OFFICER	(b)(6)

d. ADDRESS *(Include ZIP Code)*	17. REQUIRED DISTRIBUTION	
U.S. DEPARTMENT OF JUSTICE 950 PENNSYLVANIA AVE, N.W. WASHINGTON, D.C. 20530-0001	☒	a. CONTRACTOR
	☒	b. SUBCONTRACTOR
	☒	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE (b)(6)	☐	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	☒	e. ADMINISTRATIVE CONTRACTING OFFICER
	☒	f. OTHERS AS NECESSARY

DD FORM 254 (BACK), DEC 1999

Attachment to DD 254 Form For
Verint Technology, Inc.
Contract No. # DJD-13-C-0016

1. Contractor will comply with all aspects of the National Industrial Security Program Operating Manual (NISPOM and any subsequent security guidance for the protection of CLASSIFIED NATIONAL SECURITY INFORMATION (NSI).

2. Personnel security clearances at the SECRET level are required of personnel assigned to this contract.

3.This contract is for information technology support in secure buildings and contractor will not generate, store, or receive NSI material.

4. Control and protection of sensitive but unclassified information (SBU) must meet the requirements set forth in Order DOJ 2620.7 (copy attached), or its successor. At a minimum, SBU information shall be stored in a locked desk, file cabinet or similar container. Contractor shall protect all SBU information received under this contract from unauthorized disclosure.

5. Telecommunications and Automated Information Systems used to process, store, or transmit unclassified information must meet the requirements set forth in "Information Technology Security," Order DOJ 2640.2F (copy attached), or its successor. Non-US citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems, unless a waiver has been granted by the Head of the Component, with the concurrence of the DSO and the CIO.

6. All information will immediately be returned to the appropriate U.S. Government authority upon request or upon completion of the contract.

7. The DOJ has requested the Defense Security Service (DSS) provide the DOJ Special Security Center with copies of each DSS inspection report related to this contract.

8. The contractor will fully cooperate with DSS which will be conducting a review of contractor operations to be used in the performance of this contract.

9. Questions concerning the security guidance contained in this document may be directed to the DOJ SSC on 202-514-37

DOJ DOJ 2620.7

CONTROL AND PROTECTION OF LIMITED OFFICIAL USE INFORMATION

Approval Date: September 1, 1982

Approved By: KEVIN D. ROONEY
Assistant Attorney
General
for Administration

Distribution: BUR/H-1; OBD/H-1;
OBD/F-1

Initiated By: Justice Management
Division
Security Staff

1. **PURPOSE** . This order establishes Department of Justice (DOJ) regulations requiring the identification, with the marking "Limited Official Use", and the safeguarding of unclassified but sensitive information which must be protected against unauthorized disclosure. The order includes minimum protection requirements and recommends additional security safeguards to be applied where warranted by the sensitivity of the information.
2. **SCOPE**. This order applies to all organizations within the Department of Justice.
3. **REFERENCES**.
   a. 26 U.S.C. Section 6103, Publicity of returns and disclosure of information as to persons filing income tax returns.
   b. Federal Rules of Criminal Procedure, Rule 6(e), Grand Jury Secrecy of Proceedings and Disclosure.
4. **BACKGROUND**. In contrast with many government agencies, the Department of Justice has not previously issued a published policy for protecting unclassified information which is considered sensitive. Within the Department, a number of bureaus, offices, boards and divisions have issued directives or established procedures to protect sensitive information within their purview. The lack of a Department order specifying a single term to identify sensitive information throughout the Department and setting minimum protection requirements decreases the effectiveness of the individual directives or procedures when the information is released to other organizations within the Department. Additionally, the protection of sensitive information on Department wide facilities

such as the Justice Data Management Service or the Justice Telecommunications System is more difficult to effect without uniform Department policy.

5. **DEFINITION OF LIMITED OFFICIAL USE.**
   a. Limited Official Use information is unclassified information of a sensitive, proprietary or personally private nature which must be protected against release to unauthorized individuals, and this term is prescribed for use within the Department to signify such information. Information which impacts on the national security of the United States and is classified Confidential, Secret or Top Secret under Executive Order 12356 is not to be considered as Limited Official Use.
   b. The determination of categories or types of information within an organization of the Department which are considered as Limited Official Use will be the responsibility of the heads of Offices, Boards, Divisions and Bureaus (hereinafter referred to as Departmental organizations). Information must not be designated as Limited Official Use to conceal inefficiency, misdeeds or mismanagement.
   c. The following categories are provided for illustrative purposes only as examples of the types of information that Departmental organizations may want to include as Limited Official Use information:

      (1) Informant and witness information;

      (2) Grand Jury information subject to paragraph 3b;

      (3) Investigative material;

      (4) Tax information subject to paragraph 3a;

      (5) Information that could be sold for profit;

      (6) Personal information subject to the Privacy Act of 1974;

      (7) Reports that disclose security vulnerabilities;

      (8) Information that could result in physical risk to individuals;

      (9) Company proprietary information.

      (10) Deliberative information relating to internal DOJ or Executive Branch policy
      and decision making.

6. **POLICY.**
   a. The Department of Justice has access to a considerable amount of unclassified information which must be safeguarded to comply with existing laws and regulations or to protect individual rights or critical

operations of the Department or the integrity of the policy making process. It is the policy of the Department to comply with these laws and regulations and provide adequate protection to safeguard sensitive information.

b. It is the policy of the Department to comply with requests for public access to information in accordance with existing laws and regulations.

7. **RESPONSIBILITIES.**

a. Heads of Departmental organizations are responsible for ensuring compliance with this Order, specifically including:

(1) Issuing directives, if needed, establishing criteria for identifying Limited Official Use information within their organization in accordance with paragraph 5.

(2) Ensuring that adequate security measures and procedures are implemented to protect Limited Official Use information.

(3) Protecting material identified as Limited Official Use received from other organizations within the Department.

(4) Ensuring that employees of their organization are aware of their responsibility to protect Limited Official Use information.

(5) Providing the Assistant Attorney General for Administration with a copy of any implementing directive which lists the categories of information included under Limited Official Use to ensure that the categories are consistent with DOJ policy.

b. The Department Security Officer is responsible for reviewing compliance with this order and for providing guidance to Departmental organizations regarding identification and protection of Limited Official Use information.

8. **CROSS REFERENCES.** Departmental personnel should contact their Security Programs Manager or the Department Security Officer if copies of the non-DOJ references are needed to comply with the requirements of paragraph 13c. Field office personnel should contact their Security Programs Manager or the Department Security Officer if copies of paragraph 8a or 8f are needed.

a. Order DOJ 2640.1, Privacy Act Security Regulations for Systems of Records.

b. Order DOJ 2640.2, Automated Data Processing (ADP) Security.

c. Order DOJ 2620.5A, Safeguarding Tax Returns and Tax Return Information.
d. National Bureau of Standards Federal Information Processing Standards Publication 46, Data Encryption Standard.
e. Federal Telecommunications Standard 1027, General Security Requirements for Equipments Using the Data Encryption Standard.
f. Order DOJ 2710. 9A, Records Disposition Program.
g. 28 C.F.R. 45.735-10, Improper Use of Official Information.
h. 28 C.F.R. 16.56, Employee Standards of Conduct With Regard to Privacy.
i. 28 C.F.R. 50.2, Release of Information to Personnel of the Department of Justice Relating to Criminal and Civil Proceedings.
j. 28 C.F.R. 22.1, Confidentiality of Identifiable Research and Statistical Information.

9. **FREEDOM OF INFORMATION ACT (FOIA) AND PRIVACY ACT OF 1974**. The identification of material as Limited Official Use information has no connection with the Freedom of Information Act (5 U.S.C. 552) and cannot be used as a reason for approving or denying FOIA requests. Requests for access to Limited Official Use material will be considered in a similar manner as requests for any other Department information. Information subject to the Privacy Act (5 U.S.C. 552a) is required to be protected in accordance with paragraph 8a and may be included as Limited Official Use by the head of the organization concerned.

10. **DESIGNATING AUTHORITIES.**
    a. Heads of Departmental organizations have the authority to specify the categories or types of information, which originate in their organization or are prepared for the use of their organization, that are designated as Limited Official Use. If the sensitivity of the information requires protection in excess of the minimum levels established in this order, they should ensure that such criteria are known to all offices who have custody of the information.
    b. Heads of departmental organizations shall identify those subordinate officials who have authority to determine which information originating under their supervision or cognizance requires protection against unauthorized disclosure. The officials so designated are responsible for ensuring that personnel under their direction are aware of information that is considered Limited Official Use.

11. **IDENTIFICATION AND MARKING.** Department material which contains information that the head of the Departmental organization has determined requires protection against unauthorized disclosure must be identified as Limited Official Use to ensure that all persons having access to the information are aware of the protection requirement. The identification of Limited Official Use may be done by a marking of Limited Official Use on the first page of the material, by a notation in a covering memo, by inclusion in a category identified as Limited Official Use in an organization directive and known to all personnel handling the information, or any other method authorized by the head of the departmental organization. The purpose of identifying Limited Official Use information is to ensure that all recipients of the material are aware that the information requires

protection. The identification method selected should have a minimal effect on the operational efficiency of the organization.

12. **CUSTODY AND STORAGE.**
    a. Personnel who have custody of material designated as Limited Official Use shall exercise due caution to ensure that the information is not available to individuals who have no requirement for it. At a minimum, unauthorized individuals must not be able to enter areas unobserved and have visual access to Limited Official Use information.
    b. During non-duty hours, Limited Official Use material shall be afforded minimum protection of storage in a locked desk or file cabinet, or storage in a facility or area using physical access control measures which afford adequate protection to prevent unauthorized access. The sensitivity of some Limited Official Use material may require a higher level of protection such as a safe with a combination lock.
    c. Limited Official Use information stored and processed by an ADP facility shall have adequate physical, administrative and technical safeguards in accordance with paragraph 8b. Tax information must be protected in accordance with paragraph 8c.
13. **DISSEMINATION AND TRANSMISSION.**
    a. Information which has been identified and is known by the recipient as Limited Official Use shall be safeguarded from disclosure to unauthorized individuals whether or not the material is physically marked. Safeguarding from disclosure includes precautions against oral disclosure, prevention of visual access to the information and precautions against release of the material to unauthorized personnel.
    b. Limited Official Use information leaving the control of the originating organization must be transmitted in a single opaque envelope or in a wrapping properly sealed and addressed.
    c. Electronically transmitted messages or data containing Limited Official Use information shall be preceded by the term Limited Official Use at the beginning of the text. If data encryption techniques are employed, the equipment must use the Data Encryption Standard algorithm (paragraph 8d) and meet the Federal Telecommunications Standard 1027 (paragraph 8e), or be approved for National Security Information.
    d. An ADP facility handling Limited Official Use information or a remote facility used to access Limited Official Use information from an ADP system via communications links shall implement procedures to protect the information in accordance with paragraph 8b. The managers of sensitive systems accessed via communications links must consider the threats to the data in determining whether security measures such as data encryption, use of dedicated lines, terminal or user identifiers, or control and marking of output should be implemented.
    e. Limited Official Use information may be discussed on the telephone; however, the ease of interception of telephone conversations dictates that discretion be used where the threat of interception exists. In the latter case,

the use of voice privacy equipment or secure telephones should be considered.

14. **CONTRACTOR PERSONNEL**. If Limited Official Use information must be released to nongovernment personnel as part of a contract or grant, the head of the Departmental organization shall determine if the sensitivity of the information justifies a requirement for an investigation of contractor personnel handling the sensitive information. The procurement document must include the contractor background investigation requirements and other security requirements of the contract. The Security Programs Manager of the Departmental organization requesting the contract shall (1) determine the extent of the investigation required, ranging from FBI name and fingerprint checks to full-field background investigations, and (2) develop the mandatory security requirements for the contract. The contractual security requirements shall be forwarded to the Departmental organization's Security Programs Manager for concurrence prior to submitting the solicitation document to the procurement office.
15. **DESTRUCTION**.
    a. Record material may not be destroyed without appropriate disposition authority. (See paragraph 8f.) When such authority exists, physical destruction may be accomplished in the manner described in the succeeding paragraphs.
    b. Where appropriate, Limited Official Use material may be destroyed by tearing it into small pieces and discarding with other waste material. Material of higher sensitivity must be destroyed by shredding or other methods such as burning or pulping. Small segments of microfiche and microfilm may be readable; therefore, destruction into very small particles or strips is necessary.
    c. ADP storage media containing Limited Official Use data should be overwritten with nonsensitive data prior to release of the storage media. Storage media containing data of greater sensitivity should be degaussed, sanitized and/or destroyed.
16. **ADDITIONAL PROTECTION REQUIREMENTS**. The safeguards prescribed in this order are minimum requirements except where otherwise noted. The sensitivity of the information and threats to it should be considered in determining the adequacy of existing safeguards and the need for additional security protection.
17. **MATERIAL PROM OTHER DEPARTMENTS**. A number of government agencies have issued regulations for protecting sensitive information using designations such as For Official Use Only or Limited Official Use. Sensitive material from other government agencies or proprietary information from private concerns should be safeguarded from unauthorized disclosure in accordance with this order or provided additional protection in accordance with the specific requirements of the agency providing the sensitive information.
18. **UNAUTHORIZED DISCLOSURE**. Heads of Departmental organizations shall ensure that prompt and appropriate administrative action is taken against personnel responsible for disclosure of Limited Official Use material to

unauthorized individuals and issue appropriate directives, if needed, to effect this action.

/s/KEVIN D. ROONEY
Assistant Attorney General
for Administration

DOJ 2640.2F

INFORMATION TECHNOLOGY SECURITY

Approval Date: November 26, 2008

Approved By: LEE J. LOFTHUS
Assistant Attorney General for Administration

Distribution: BUR/H-1; OBD/H-1; SPL-23

Initiated By: Department Chief Information Officer

FOREWORD

1. **PURPOSE.** This order establishes uniform policy, responsibilities and authorities for protection of Information Technology (IT) systems that store, process or transmit Department of Justice (Department) information.

2. **SCOPE.** The provisions of this order apply to all Department Components, personnel and IT systems used to process, store or transmit Department information. They apply to contractors and other users of IT systems supporting the operations and assets of the Department, including any non-Department organizations and their representatives who are granted access to Department IT resources, such as other Federal agencies. This policy applies to IT systems processing National Security Information and unclassified information.

3. **CANCELLATION.** Department Order 2640.2E is cancelled.

4. **AUTHORITIES.** The Department Chief Information Officer (CIO) is responsible for providing policy, guidance, implementation and oversight for IT systems.

5. **REPERCUSSIONS FOR COMPONENT NON-COMPLIANCE.** The Department CIO may take appropriate action if a Component, contractor or other non-Department organization or their representatives are found to be non-compliant with Department IT security policy. The Department Chief Information Security Officer (CISO), and Department Security Officer (DSO) shall be notified in cases of such non-compliance in order to take appropriate action.

6. **REFERENCES.** References to various regulations and laws applicable to the responsibilities of IT security are located in APPENDIX 1. Future updates to referenced documents will be considered applicable to this order.

7. **DEFINITION OF TERMS.** Terms shall have the meaning defined by National Institute of Standards and Technology Interagency Reports (NISTIRs), Federal Information Processing Standards (FIPS) and Special Publications (SP). Unless otherwise stated, all terms used in NIST publications are also consistent with the definitions contained in the Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary.

/s/LEE J. LOFTHUS
Assistant Attorney General
for Administration

TABLE OF CONTENTS

CHAPTER 1. INFORMATION TECHNOLOGY SECURITY POLICY

1. Component Information Technology Security Programs.

Each Component shall establish and maintain an IT security program, in compliance with the Department's overall IT security program, to ensure the confidentiality, integrity and availability of the Component's computer systems, networks and data, in accordance with all Federal and Department policies, standards, procedures and guidance.

2. Required Use of DOJ IT Systems

DOJ information used for official business may only be processed, stored, or transmitted on IT systems meeting the requirements of this order.

This restriction does not apply to DOJ information disseminated to other Federal, State, Local or Tribal agencies, or to information released to the public or as part of a court proceeding, or to information whose release is required to accomplish a non-DOJ function (e.g., information released to a hospital so it can provide health care services to a prisoner).

3. Management Security Policy

a. **Risk Assessment.** In accordance with DOJ IT Security Standard - Risk Assessment (RA) Control Family, Components shall periodically assess the risk to Departmental operations (including mission, function, image or reputation) and assets, individuals, other organizations, and the Nation resulting from the operation of Department IT systems and the associated processing, storage, or transmission of Department information.

b. **Planning.** In accordance with DOJ IT Security Standard – Planning (PL) Control Family, Components shall develop, document, periodically update and implement security plans for Department IT systems that describe the security controls in place or planned for the IT systems and the rules of behavior for individuals accessing the IT systems.

c. **System and Services Acquisition.** In accordance with DOJ IT Security Standard - System and Services Acquisition (SA) Control Family, Components shall:

(1) Allocate sufficient resources to adequately protect Department IT systems.

(2) Employ systems development life cycle processes that incorporate IT security considerations.

(3) Ensure new acquisitions include available Commonly Accepted Security Configurations.

(4) Perform acquisition risk assessments, and develop and adopt effective supply chain risk mitigation for IT acquisitions.

(5) Employ software usage and installation restrictions to ensure software installed on Component IT systems is in compliance with applicable copyright laws and licensing agreements.

(6) Ensure third-party providers are contractually required to comply with this policy to employ adequate security measures to protect information, applications and/or services outsourced from the Department.

d. **Certification, Accreditation and Security Assessments.** In accordance with DOJ IT Security Standard – Certification, Accreditation and Security Assessments (CA) Control Family, Components shall:

(1) Periodically assess the security controls in Component IT systems to determine if the controls are effective in their application.

(2) Develop, monitor and implement plans of action and milestones (POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in Component IT systems.

(3) Authorize the operation of Component IT systems and any associated IT system interconnections prior to operational use, and notify the Component CIO.

(4) Monitor IT system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

4. Operational Security Policy

a. **Personnel Security.** In accordance with DOJ IT Security Standard – Personnel Security (PS) Control Family, Components shall:

(1) Ensure individuals occupying positions of responsibility within the Component (including third-party service providers) are trustworthy and meet established security criteria for those positions.

(2) Ensure Non-United States (U.S.) citizens are not authorized to access or assist in the development, operation, management or maintenance of Component IT systems, unless a waiver has been granted by the Component Head, with the concurrence of the Department Chief Information Officer (CIO) and Department Security Officer (DSO).

(3) Ensure Component information and IT systems are protected during and after personnel actions such as terminations and transfers.

(4) Employ formal sanctions for personnel failing to comply with Department security policy and procedures.

b. **Physical and Environmental Protection.** In accordance with DOJ IT Security Standard – Physical and Environmental Protection (PE) Control Family, Components shall:

(1) Limit physical access to IT systems, equipment and the respective operating environments to authorized individuals and monitor and log all such accesses.

(2) Protect the physical plant and support infrastructure for IT systems.

(3) Provide supporting utilities for IT systems.

(4) Protect IT systems against environmental hazards.

(5) Provide appropriate environmental controls in facilities containing information systems.

c. **Contingency Planning.** In accordance with DOJ IT Security Standard – Contingency Planning (CP) Control Family, Components shall establish, maintain and effectively implement plans for emergency response, backup operations and post-disaster recovery for Component IT systems to ensure the availability of critical IT resources and continuity of operations in emergency situations.

d. **Configuration Management.** In accordance with DOJ IT Security Standard – Configuration Management (CM) Control Family, Components shall:

(1) Establish and maintain baseline configurations and inventories of Component IT systems (including hardware, software, firmware and documentation) throughout the respective system development life cycle.

(2) Establish a configuration change control process to ensure proposed changes are evaluated, tested, properly approved and documented before being put into production.

(3) Establish and enforce security settings consistent with the information system operational requirements and Department commonly accepted security configurations (e.g., Federal Desktop Core Configuration) and validate those controls through Department approved tools.

e. **Maintenance.** In accordance with DOJ IT Security Standard – Maintenance (MA) Control Family, Components shall:

(1) Perform periodic and timely maintenance on Component IT systems.

(2) Provide effective controls on the tools, techniques, mechanisms and personnel used to conduct on-site and remote IT system maintenance.

f. **System and Information Integrity.** In accordance with DOJ IT Security Standard – System and Information Integrity (SI) Control Family, Components shall:

(1) Identify, report and correct information and information system flaws in a timely manner.

(2) Provide protection from malicious code at appropriate locations within Component IT systems.

(3) Monitor IT system security alerts and advisories and take appropriate actions in response.

g. **Media Protection.** In accordance with DOJ IT Security Standard – Media Protection (MP) Control Family, Components shall:

(1) Protect IT system media, both paper and digital.

(2) Encrypt sensitive and classified information transported outside of the agency's secured, physical perimeter in digital format (including information transported on removable media such as USB drives, CDs, DVDs and on portable/mobile devices such as laptop computers and/or personal digital assistants) using FIPS 140-2 validated or NSA approved encryption, as appropriate.

(3) Limit access to information on IT system media to authorized users.

(4) Sanitize or destroy IT system media before disposal or release for reuse.

(5) Stipulate in contracts for equipment maintenance warranty that equipment to be removed from the Component's physically protected offices shall be sanitized before removal.

h. **Incident Response.** In accordance with DOJ IT Security Standard – Incident Response (IR) Control Family, Components shall:

(1) Establish an operational incident handling capability for Component IT systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities in coordination with the Department of Justice Computer Emergency Response Team (DOJCERT).

(2) Track, document and report incidents to appropriate Department officials and/or authorities.

(3) Provide Department forensics and law enforcement personnel access to media and devices required for investigation, when appropriate.

(4) Assist with digital forensics on electronic devices and/or associated media.

(5) Maintain a chain of custody to record the handling and transfer of media and devices to support investigations and forensics.

i. **Awareness and Training.** In accordance with DOJ IT Security Standard – Awareness and Training (AT) Control Family, Components shall:

(1) Ensure managers and users of Component and Department IT systems are aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policy, standards, instructions, regulations, or procedures related to the security of Component and Department IT systems and data, including digital and paper.

(2) Ensure Component personnel are adequately trained to carry out their assigned IT security-related duties and responsibilities.

5. **Technical Security Policy**

a. **Identification and Authentication.** In accordance with DOJ IT Security Standard – Identification and Authentication (IA) Control Family, Component IT systems shall:

(1) Identify IT system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Component IT systems.

(2) Allow remote access only with two-factor authentication where one factor is provided by a device separate from the computer gaining access. (See Chapter 2, paragraph 13)

b. **Access Control.** In accordance with DOJ IT Security Standard – Access Control (AC) Control Family, Component IT systems shall:

(1) Limit IT system access to authorized users, processes acting on behalf of authorized users, or devices (including other IT systems) and to the types of transactions and functions authorized users are permitted to exercise.

(2) Restrict remote access to Government or contractor owned systems. Remote access from personally owned and "public computers" is prohibited. (See Chapter 2, paragraph 13)

(3) Prohibit automatic forwarding of email received in a Component or Department email system to or through a non-Department email system, unless the Authorizing Official grants a waiver.

c. **Audit and Accountability.** In accordance with DOJ IT Security Standard – Audit and Accountability (AU) Control Family, Component IT systems shall:

(1) Create, protect and retain IT system audit records to the extent needed to enable security monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate IT system activity.

(2) Ensure the actions of individual IT system users can be uniquely traced to those users so they can be held accountable for their actions.

(3) Provide direct, real-time or near real-time electronic data feeds of all relevant security monitoring and auditing data (e.g., Firewall event logs, Intrusion Detection or Prevention system alerts and logs, network and desktop antivirus event logs, content scanning and filtering system logs, DHCP, DNS, etc.) to the Department Security Operations Center (SOC) systems unless the Department CIO grants a waiver based upon assessed risk, mitigating controls and operation requirements.

d. **System and Communications Protection.** In accordance with DOJ IT Security Standard – System and Communications Protection (SC) Control Family:

(1) All connections to external networks supporting external access and/or remote access to Department or Component IT systems shall be obtained through a Trusted Internet Connection Access Provider (TICAP), unless the Department CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.

(2) The Department shall maintain and publish a list of known malicious resources and sites. Components shall implement blocking of these resources and sites at boundary protection devices. Exceptions to allow access to resources and/or sites on this list must be approved by the Component CIO and reported to the Department's Security Operations Center.

(3) Components shall monitor, control and protect Component communications (e.g., information transmitted or received by Component IT systems) at the external boundaries and key internal boundaries of the IT systems.

(4) Component systems shall utilize approved cryptographic mechanisms or protected distribution systems to protect the confidentiality and integrity of information transmitted beyond the secured physical perimeter.

(5) Remote access computers shall use an encrypted VPN to connect to Component information systems.

(6) Components shall employ architectural designs, software development techniques and systems engineering principles that promote effective IT security within Component IT systems.

(7) Components shall be prohibited from deploying systems, technologies, or services (e.g., encapsulation, tunneling, encryption) inconsistent with department security enterprise architecture requirements (e.g., Firewalls, Intrusion Detection Systems, Antivirus systems, content scanning and filtering systems), unless the Department CIO grants a waiver based upon assessed risk, mitigating controls, and operational requirements, prior to operational use.

6. National Security Systems and Sensitive Compartmented Information (SCI) IT Systems

Security policy for systems processing collateral (i.e., non-SCI) national security information is established by the Committee on National Security Systems (CNSS). Security policy for systems processing Sensitive Compartmented Information (SCI) is established by Director of National Intelligence (DNI) in Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation. The Department Security Officer (DSO) is responsible for obtaining accreditation of IT systems processing SCI.

Components shall conform to DOJ Security Program Operating Manual (SPOM), ICD 503 and CNSS policies to manage the security of their National Security Systems. Components shall use NIST SP 800-59, "Guideline for Identifying an Information System as a National Security System." to identify National Security Systems.

7. Classified Laptop and Mobile Computing Devices

The Department Security Officer (DSO) and Department Chief Information Officer (CIO) shall approve, in writing, the processing of classified information on laptops and mobile computing devices. Requests for approval shall be submitted through the Chief Information Security Officer who will obtain the approvals. DOJ IT Security Standard – Classified Laptop and Standalone Computers Security Policy outlines the requirements for laptop computers that process or store classified information, including requirements for standalone computers that process or store classified information.

8. Use of DOJ IT Resources Outside US Territory.

The Department Security Officer (DSO) and Department Chief Information Officer (CIO) shall approve, in writing, the transportation or use of DOJ computers outside of US Territory. Components may approve the use of Department telephones, including BlackBerry smartphones and similar devices, outside US Territory. Components shall:

a. Limit data taken outside US Territory to that which is needed to accomplish the purpose of the travel.

b. Prevent remote access to DOJ IT systems from outside US Territory, with the exception of systems specifically accredited for such access and email via smartphones or personal digital assistants (PDAs).

c. Inspect computers, smartphones, PDAs and media that have been transported outside US Territory for compromise prior to any physical connection to a Component or Department system. If the Component can not conduct such an inspection, it shall reimage the computer or sanitize the media.

9. Facsimile

a. All classified and sensitive facsimile transmissions shall be preceded by a cover sheet containing the following information:

(1) The classification or sensitivity of the information.

(2) The name, office and voice/fax telephone numbers for the recipient(s) and sender.

(3) A warning banner with instructions to the recipient if the facsimile was received in error.

b. Classified information shall be encrypted for transmission with National Security Agency (NSA)-approved encryption.

CHAPTER 2. ISSUE-SPECIFIC SECURITY POLICIES

Whereas program policy is intended to address the broad organization wide computer security program, the issue-specific policies in this chapter focus on areas of current relevance and concern to the Department.

10. Sensitive and Personally Identifiable Information (PII)

The term "personally identifiable information" refers to information that can be used to distinguish or trace individuals' identity, such as their name, social security number, biometric records, etc. 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, mother's maiden name, etc. Loss or disclosure of sensitive information not only has a serious negative impact on our law enforcement and other critical functions, but also diminishes the public trust in our operations. There is inherent risk in carrying such data on mobile computers and devices. The purpose of this policy is to compensate for the lack of

physical security controls when information is removed from or accessed from outside the agency location. Components shall:

a. Reduce the volume of collected and retained PII to the minimum necessary.

b. Limit access to only those individuals who must have such access.

c. Categorize sensitive PII and information systems processing such information as moderate or high impact.

d. Not remove sensitive PII from Component controlled IT systems or facilities unless required (e.g., court filings, debt collection activities).

e. Log all computer-readable data extracts from databases holding sensitive information and ensure each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is considered sensitive information unless designated as non-sensitive by the Component head.

f. Notify the DOJ Computer Emergency Readiness Team (DOJCERT) of all incidents involving known loss of sensitive data and PII as an Unauthorized Access incident (Category 1) within one hour of discovery. Loss of any data storage devices, such as laptops, flash drives, disks and tapes, should be reported as an Incident under Investigation (Category 6) within the same one hour time frame. DOJCERT will notify the US-CERT and the Department CIO.

g. Ensure all contracts involving the processing and storage of PII comply with Department policies on remote access and security incident reporting.

11. External Information Systems

External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the Component and for which the Component typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External access includes interconnections between Department IT systems and non-Department IT systems, and between Component IT systems internal to the Department, where there is direct connection of two or more IT systems for the purpose of sharing data and other information resources. External access also includes connections to the Internet.

External access presents both security concerns and resource management issues. The goal of this policy is to ensure Components can effectively, efficiently and safely exchange data with other government and private sector systems, and can utilize resources available on the Internet to accomplish their missions.

Components shall:

a. Obtain all connections to external networks that support external access and/or remote access through a Trusted Internet Connection Access Provider (TICAP), unless the Department CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.

b. Be prohibited from deploying systems, technologies, or services (e.g., encapsulation, tunneling, encryption, etc) inconsistent with department security architecture requirements (e.g., Firewalls, Intrusion Detection or Prevention Systems, Antivirus systems, content scanning and filtering systems, etc.), unless the Department CIO grants a waiver based upon assessed risk, mitigating controls, and operational requirements, prior to operational use.

12. Protection of Mobile Computers/Devices and Removable Media

Information physically transported outside of the Department's secured physical perimeter is more vulnerable to compromise. The intent of this policy is to compensate for the protections no longer offered by the physical security controls when information is removed from the Component location.

Information on mobile computers/devices (e.g., notebook computers, personal digital assistants) and removable media shall be encrypted using FIPS 140-2 validated or NSA approved encryption mechanism, based on the classification of information processed on the device; unless the data is determined to be non-sensitive, in writing, by the Component Head or principal deputy. Mobile computers shall utilize anti-viral software and a host-based firewall mechanism. Components shall ensure all security related updates are installed on mobile computers/devices. Information should be deleted from mobile computers/devices when no longer needed.

13. Remote Access to DOJ Systems

Remote access is any access to a Component's nonpublic information system by a user (or an information system) communicating through an external, non-Department-controlled network (e.g., the Internet) using a Component controlled computer. Remote access presents additional security concerns since the Component has no direct control over the application of required security controls or the assessment of security control effectiveness of the connecting network. The goal of this policy is to ensure Components can safely utilize remote access to better accomplish their missions.

a. Remote access systems shall be restricted to Government owned or contractor owned systems. Remote access from personally owned or "public computers" is prohibited.

(1) Remote computers shall employ anti-viral software, firewalls and encryption of stored data using FIPS 140-2 validated or NSA approved encryption.

(2) Remote computers shall have all current and applicable Operating System (OS) and application security updates in place.

(3) Components shall utilize a configuration management system for remote access computers to ensure the remote access computer has the Component approved security software in place, the OS is fully patched, antivirus software is installed and up-to-date and a personal firewall is enabled.

(4) Remote access computers shall use two-factor authentication where one factor is provided by a device separate from the computer gaining access.

(5) Remote access computers shall use an encrypted VPN to connect to Department information systems.

(6) Remote access computers shall not be connected to any other network when connected to a Department IT system.

(7) Remote access login sessions shall be restricted to a single operating system and a single network interface card when connected to a Department IT system.

14. Contractors

The Components and Department may utilize contractors to develop, operate and/or maintain IT systems on their behalf. Contractors may be granted access to Component and Department IT systems and information in order to perform work specified under the contract. Access may be from Component or Department owned computers or from contractor owned computers. Contractors may process Component and Department information on contractor owned equipment, either within or outside DOJ space. In all these situations, the contractors and their sub-contractors, their personnel and their IT systems and devices shall fall under the provisions of this order, and the contract shall identify IT security requirements.

All connections to external networks supporting access to DOJ hosted resources (e.g., Government owned web sites, applications, email systems) shall be obtained through a Trusted Internet Connection Access Provider (TICAP), unless the Department CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.

When the contract requires or allows contractor IT systems to be used, whether to access Component or Department IT systems and/or information or to process or store Component or Department information, the contract shall require the contractor IT systems be certified, accredited and operated pursuant to a valid Authority to Operate (ATO). The ATO shall be issued by a Component Authorizing Official based on this policy. If the contractor utilizes its own internal C&A process it must submit the C&A package to the Component Authorizing Official. If the Component Authorizing Official determines the C&A process

meets the Department standards, he or she may issue an ATO based on the package. Contractors using individual devices under the contract shall provide the Contracting Officer's Technical Representative (COTR) an inventory of such devices and shall operate such devices pursuant to this policy, including all incident response requirements. Contractors and contractor systems shall be subject to the same FISMA data calls as other DOJ systems.

Upon termination of contract work, all DOJ information shall be removed from contractor owned IT equipment. Certification of data removal shall be performed by the contract's project manager and a letter confirming certification shall be delivered to the Contracting Officer within 15 days of the termination of the contract.

CHAPTER 3. DETERMINING SECURITY CONTROL REQUIREMENTS

15. Applicability

The standard security control requirements in this Chapter are applicable to all DOJ IT systems. DOJ IT systems that process National Security Information (NSI) must meet any additional requirements specified by the Committee on National Security Systems (CNSS). DOJ IT systems that process Sensitive Compartmented Information (SCI) must meet any additional requirements specified by the Director of National Intelligence (DNI). If there is a conflict in requirements for systems processing NSI or SCI, the CNSS or DNI requirements shall govern. Components shall use NIST SP 800-59, "Guideline for Identifying an Information System as a National Security System," to identify National Security Systems.

16. Categorize information types and information systems

a. Components shall categorize all Department IT systems as low-impact, moderate-impact, or high-impact, in accordance with Federal Information Processing Standards (FIPS) 199 and 200, or applicable standards for national security systems, as partially implemented in the Department-approved Cyber Security Assessment and Management (CSAM) Toolkit. This process establishes security categories for information types and information systems. The security categories are based on the potential impact on a Component should certain events occur that jeopardize the information and information systems needed by the Component to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals. The impact value for a system shall be the highest value (i.e., high water mark) from those determined for each type of information resident on the system.

b. The Component's risk assessment (threat and vulnerability information) and mission criticality indicators are given manual consideration regarding any required adjustments in the categorization results. Rationale for deviations from the recommended security categorizations must be documented in the System Security Plan. Designated senior-level

officials within the Component shall review and approve the security categorizations. Documented results of this approval are captured in the System Security Plan.

17. Select, tailor and supplement initial baseline security controls

a. The Department has developed IT Security Standards based on the security control families outlined in Federal and National standards, supplemented with additional Department standards. The Department's IT Security Standards outline, in specific detail, the requirements for achieving the high-level goals within this Order. The DOJ IT Security Standards represent minimum DOJ IT security control requirements, supplement this Order and are required for use in accordance with the terms and conditions expressed in the Standards. The requirements in the Standards are implemented in CSAM.

b. Subsequent to the security categorization process, Components shall select an appropriate set of security controls and assurance requirements for their information systems that satisfy the minimum security requirements set forth in these standards and are tailored (enhanced or limited) based on the results of a risk assessment and local conditions, including Component- or system-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

c. The information system authorizing official shall determine if the control set in the information system security plan is appropriate for securing the information system to an acceptable level of operational risk to the Component. Components shall document the authorizing official's approval of the initial set of tailored security controls in the System Security Plan, including the Component's rationales for any refinements or adjustments to the baseline set of controls.

18. Implement security controls

Components shall then implement the security controls in the information system in accordance with the System Security Plan. Authorizing officials are better positioned to make mission risk determinations based on the known vulnerabilities remaining in the information system after the implementation of an agreed-upon set of security controls.

19. Assess and Authorize the implemented controls

Components shall assess the security controls using appropriate methods and procedures (e.g., CSAM) to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. The system authorizing official shall authorize the information system operation based upon a determination of the risk to Departmental operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

20. Monitor

a. Components shall monitor the information system on a continuous basis for changes to the information system or its operational environment, the information system security plan boundaries, or other conditions (e.g., threat and risk factors), conducting security impact analyses of the associated changes, updating the information System Security Plan (and other relevant information system documentation as appropriate) and report changes to the security status of the system to appropriate officials on a regular basis.

b. Significant changes to the system require reaccreditation by the information system's Authorizing Official. Examples of changes to an information system that should be reviewed for possible reaccreditation include:

(1) installation of a new or upgraded operating system, middleware component, or application;

(2) modifications to system ports, protocols, or services;

(3) installation of a new or upgraded hardware platform or firmware component; or

(4) modifications to cryptographic modules or services;

(5) additional connections to information systems outside the accreditation boundary;

(6) functional changes or enhancements to the system that affect its mission criticality, information types, user base, or classification of data supported by the information system.

c. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.

d. Reauthorization should be avoided in situations where the continuous monitoring process provides the necessary and sufficient information to authorizing officials to manage the potential risk arising from the information system changes.

CHAPTER 4. ROLES AND RESPONSIBILITIES

21. Department Chief Information Officer

Per the Clinger Cohen Act of 1996, the Chief Information Officer (CIO), who also serves as Deputy Assistant Attorney General, Information Resources Management (DAAG/IRM), advises and assists the Attorney General, the Deputy Attorney General, the Assistant Attorney General for Administration and other senior staff in order to ensure the Department

plans, acquires, manages and uses Information Technology (IT) in a manner that enhances mission accomplishment; improves work processes and reduces paperwork; provides sufficient protection for the privacy of personal information; promotes citizen-centered electronic government; and is consistent with all applicable Federal laws and directives. The Department CIO, in addition to the responsibilities outlined in Department Order 2880.1B, Information Resources Management Program, shall be responsible for:

a. Ensuring the Department's IT security program is established and implemented in compliance with Federal laws and regulations.

b. Issuing IT security policy, standards and guidelines to address IT security planning, management and implementation.

c. Developing and/or managing enterprise IT control techniques and technologies while considering Department Component infrastructure and resources and developing and/or managing enterprise security management tools.

d. Reviewing and evaluating the implementation of Department Component program and system security controls in accordance with Department's IT security policy, standards and guidelines.

e. Developing and maintaining the Department's IT Security Program Management Plan (PMP) in accordance with Federal laws and regulations.

f. Developing, implementing and managing a Department-wide Plan of Action and Milestone (POAM) process to correct IT security weaknesses.

g. Requiring Components and program officials to implement Department policy, standards and guidance in the absence of an approved waiver (where applicable), or justification for the use of compensating controls, including a formal assessment and acceptance of risk.

h. Ensuring senior agency officials provide IT security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of:

   (1) Information collected or maintained by or on behalf of the Department.

   (2) IT systems used or operated by an agency, or by a contractor of an agency, or other organization on behalf of an agency.

i. Enforcing Department IT security policy, including levying sanctions on Components for non-compliance.

j. Developing and maintaining a central repository of information on new and emerging technologies. Coordinating and approving any evaluations of new and emerging technologies by Components.

k. Coordinating with the Department Security Officer (DSO) on Sensitive Compartmented Information (SCI) IT systems.

l. Ensuring all Department personnel with access to Department networks and all individuals at contractor facilities working on Department systems, information, or providing services, receive annual IT security awareness training.

m. Ensuring IT security management processes are integrated with the Department and/or Component strategic and operational planning processes.

n. Concurring with or disapproving waiver requests relating to non-United States (U.S.) citizens accessing or assisting in the development, operation, management, or maintenance of Department IT systems.

o. Approving and monitoring waivers to IT security requirements (other than waivers relating to non-U.S. citizens accessing or assisting the development, operation, management, or maintenance of Department IT systems).

p. Approving encryption technologies that are not FIPS 140-2 validated in those situations where FIPS-validated products are not available.

q. Appointing a Chief Information Security Officer (CISO) to carry out the Department-wide IT security program as required by the Federal Information Security Management Act (FISMA).

r. Establishing an IT Security Governance Committee (ITSGC) to be chaired by the Department CIO and consisting of the Deputy Department CIOs and selected Component CIOs. The ITSGC shall be the focal point for providing strategic direction on Department level initiatives.

s. Establishing an IT Security Council (ITSC) with supporting project teams composed of lead-Component IT security personnel.

t. Reporting to the Attorney General and Office of Management and Budget (OMB) on the status of the Department's IT Security Program.

22. Chief Information Security Officer

The Chief Information Security Officer (CISO) chairs the Department's ITSC and serves as the principal security leader for the Department to implement the requirements of FISMA. The CISO also serves as the Department CIO's liaison to Federal agencies for all matters

relating implementation of IT security and the Department's IT Security Program. The Department CISO shall be responsible for:

a. Developing standards and guidelines for conducting risk assessments to assess risk and determine needs.

b. Implementing Department-wide policy and procedures for related controls to cost-effectively reduce risks to an acceptable level.

c. Monitoring, evaluating and periodically testing IT security controls and techniques to ensure they are effectively implemented.

d. Developing and maintaining a Department-wide IT security program.

e. Providing leadership for the ITSC to execute Department-wide management and implementation of the Department's IT security program.

f. Identifying and developing common security controls and managing the implementation and assessment of common security controls.

g. Ensuring and promoting a comprehensive IT security training program for both privileged and general users.

h. Assessing waiver requests for Department's IT Security Standards on behalf of the Department Chief Information Officer (CIO).

i. Preparing the annual and quarterly Federal Information Security Management Act (FISMA) reports for the Department CIO.

j. Ensuring compliance with monthly reporting on the effectiveness of Component IT security programs, including progress of remedial actions.

k. Identifying IT security management and reporting tools through the IT Security Council (ITSC) for use throughout the Department.

l. Assisting senior Department Component IT security officials in their responsibilities through the ITSC.

23. Department Security Officer

The Department Security Officer (DSO) conducts security compliance reviews to assess the overall effectiveness of security program implementation across the Department, including IT security. The DSO ensures all IT security reviews that require system testing are coordinated with the Department CIO and all IT security-related findings are reported to the Department CIO. The DSO shall be responsible for:

a. Providing advice to the Department CIO on security program areas affecting IT.

b. Providing advice and recommendations to the Department CIO on waiver requests.

c. Concurring with or disapproving requests for waivers relating to non-United States (U.S.) citizens accessing or assisting in the development, operation, management, or maintenance of Department IT systems.

d. Ensuring the development and implementation of Department-wide policy and procedures to govern: TEMPEST; Technical Surveillance Countermeasures (TSCM); Personnel Security; Physical and Environmental Security; Storage and Marking; Media Disposal; Media Reuse; Communications Security (COMSEC) materials; facsimile security; copier security; and those aspects of the DSO's responsibilities for Personnel Security; Document Security; Physical Security; COMSEC; and Emergency Planning described in Department Order 2600.2C.

24. Component Heads or Their Designee(s)

The Component Head or his/her designee(s) shall establish and maintain a Component-wide IT security program to secure the Component's IT systems, networks and data in accordance with Department policy, procedures and guidance. The Component Head or designee(s) work with the Department Chief Information Security Officer (CISO) through the IT Security Governance Committee and IT Security Council to carry out the following responsibilities at the Component level:

a. Implementing Department policy, standards and guidelines.

b. Implementing the Department's IT Security Program Management Plan at Component and system level, and reporting results in accordance with Office of the CIO (OCIO) guidelines.

c. Ensuring the completion of monitoring, testing and evaluation of the effectiveness of IT security policy, procedures, practices and security controls to be performed with a frequency depending on risk, as directed by ITSS.

d. Ensuring the completion of periodic assessments of risk, including the magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and IT systems that support the operations and assets of the Department.

e. Developing, implementing, managing and prioritizing corrective plans of actions and milestones to correct known weaknesses in IT security using the department-wide POAM process.

f. Reporting quarterly in accordance with guidance issued by Justice Management Division (JMD) or the Department CIO, on the status of their IT security programs to the Department CIO and CISO.

g. Integrating security in the Capital Planning Investment Control (CPIC) process.

h. Assigning roles and responsibilities within the Component (e.g., Component ITSC member, Component CIO, Authorizing Official, Certification Agent, Information System Owner, Information Owner, User Representative, Information System Security Officer).

i. Coordinating with the OCIO any evaluations of new technologies that could impact Department or enterprise services.

j. Participating with other Components and the OCIO in evaluating and selecting IT security tools for use within the Department and obtaining Department CIO approval for non-enterprise IT security solutions.

k. Establishing procedures to ensure software installed on Component IT systems is in compliance with applicable copyright laws and is incorporated into the IT system's life cycle management process.

l. Approving, with the concurrence of the Department CIO and Department Security Officer (DSO), waivers relating to non-United States (U.S.) citizens accessing or assisting in the development, operation, management, or maintenance of Department IT systems, and monitoring those waivers.

m. Ensuring all Component personnel with access to Department networks and all individuals at contractor facilities working on Department systems, information, or providing services, receive annual IT security awareness training.

CHAPTER 5. AGENCY-WIDE PROGRAM IMPLEMENTATION

25. Core Program

a. The Department shall develop and manage an agency-wide IT Security Program, executed through the Department's IT Security Program Management Plan (PMP), consistent with the laws and regulations affecting IT security. The Department's IT security management approach shall employ a collaborative and coordinated effort to maximize available resources and protect Department IT systems and operations.

b. The Department Chief Information Officer (CIO) shall establish security governance through the use of appropriate committees to provide a systematic forum to assist in the accomplishment of established Department IT security objectives.

26. IT Security Management Strategy

The IT security management strategy used by the Department shall be based on the risk management concepts found in Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems," the Federal Information Security Management Act (FISMA), and other Federal guidance. The risk management principles in the proceeding sections provide the framework for the Department's IT security management strategy. An important factor in effectively implementing these principles is linking them in a cycle that ensures IT security policy addresses current risks on an ongoing basis.

a. Central Focal Point

The Information Technology Security Staff (ITSS) shall serve as the central focal point for IT security in the Department. The ITSS shall provide Department-wide management and implementation of the Department IT security program. The ITSS and the Components shall provide a collaborative team to manage the accomplishment of priorities for achieving business objectives and complying with FISMA; Homeland Security Presidential Directives; Presidential Decision Directives/ Presidential Directives; Executive Orders; Office of Management and Budget (OMB); National Institute of Standards and Technology (NIST); Committee on National Security Systems (CNSS); Director of National Intelligence (DNI) Directives; and Department IT security requirements.

b. Follow a Department-wide common Security Strategy

The Department shall follow a common Security Strategy that defines the common security goals for all Components. These goals shall outline the Department's security posture both internally and externally while taking into account the respective business needs and missions of each Component. The Department's common Security Strategy will be strengthened by the adoption of a common IT Security Architecture developed to ensure information systems remain secure throughout their entire lifecycle. The security needs and requirements shall be identified early on in the process and be funded appropriately.

c. New and emerging technologies

Information technology is a dynamic field with new and emerging technologies constantly being identified that could assist the Department to better accomplish its constantly evolving mission. The OCIO shall provide a central repository of information on these technologies. Components shall coordinate with this office prior to undertaking any evaluation of new or emerging technologies. This office shall maintain all evaluations and make them available to Components to leverage work already performed and to avoid duplication of effort.

d. Implement Policy and Procedures

(1) The Department's IT Security policy shall clearly address the Department's IT security needs and serve as the foundation for the Department's IT security program. Policy shall represent the primary mechanism for senior management to communicate its IT security requirements to the Components. Policy shall be adjusted (as required) and shall be related to the risk of the Department or Components not being able to perform their functions.

(2) The Department's IT Security Standards shall provide detailed procedures for implementing Department policy and shall be practical to implement. The IT Security Standards shall outline specific requirements for accomplishing the Department's security goals. The Department's IT Security Standards are divided into the following three general security control classes: (i) Management; (ii) Operational; and (iii) Technical.

e. Promote Awareness

All users of Department IT systems shall be continually educated on risks and related policy as they are more likely to support and comply with the policy if they understand the purpose behind the policy and their associated responsibilities.

f. Manage Risk and Determine Needs

(1) Senior management views IT security as an "enabler." Based on a thorough examination of the risks, Department and Component Senior management shall assume risks and take responsibility for the operation of systems based on risks identified in assessments balanced by the impact the IT system has on Department operations. Additionally, the risk management process shall be continually evaluated to ensure it addresses the current threats to Department IT systems.

(2) The Department's risk management methodology shall present a formal, structured approach for developing risk assessments for IT systems that are part of a major application or general support system. This methodology shall provide a uniform standard for evaluating IT security risks to IT systems operating within the Department. The primary focus of this methodology shall be on the IT system's mission, not IT assets. Since risk management is an essential management function, Department IT system owners and IT security managers shall use this methodology when assessing risks and prioritizing resources for certifying and accrediting Department IT systems.

g. Monitor and Evaluate

The Department's IT security program shall include continually monitoring and assessing IT security policy and IT security controls to ensure they remain appropriate and effective. Monitoring control effectiveness and compliance with policy shall be

incorporated within the cycle of managing the Department's IT security program, and shall be performed through the use of automated software tools when possible.

APPENDIX 1. REFERENCES

The following references are applicable to the Department IT security policy. Unless otherwise stated, all references to publications (e.g., NIST Federal Information Processing Standards, NIST Special Publications) are to the most recent version of the referenced publication.

1. Congressional Mandates

a. Clinger Cohen Act of 1996, (Pub. L. 104-106, 110 Stat. 186); and (Pub. L. 104-208, 110 Stat. 3009).
b. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.
c. Computer Security Act of 1987, 15 U.S.C. § 272, 278h, 278g-3, 278g-4.
d. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511.
e. E-Government Act of 2002, PL 107-347, 44 U.S.C. Ch 35.
f. Federal Information Security Management Act of 2002 (FISMA), Pub. L. 107-347, 116 Stat. 2899.
g. Federal Managers Financial Integrity Act of 1982 (FMFIA), Pub. L. 97-255, 96 Stat. 814.
h. Freedom of Information Act (FOIA), 5 U.S.C. § 552.
i. Paperwork Reduction Act of 1995 (PRA), Pub. L. 104-13, 109 Stat. 163; 44 U.S.C. 3501-3520.
j. Privacy Act of 1974, 5 U.S.C. § 552a.

2. Federal/Departmental Regulations/Guidance

a. 28 C.F.R. 45.4, Personal Use of Government Property.
b. 36 C.F.R. 1194, Electronic and Information Technology Accessibility Standards (65 FR 80500).
c. 41 C.F.R. 101-35, Telecommunications Management Policy.
d. Committee on National Security Systems Instruction (CNSSI) No. 7000, TEMPEST Countermeasures for Facilities.
e. CNSS Policy (CNSSP) No. 6, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems
f. CNSSI No. 4009 National Information Assurance Glossary.
g. CNSSI No. 4016, National Information Assurance Training Standard For Risk Analysts
h. CNSS NSS Instruction 1199, Security Categorization for National Security Systems and Information (ODNI/CIO Draft).
i. CNSS NSS Instruction 1218 (ODNI/CIO Draft), Guide for Developing Security Plans for National Security Information Systems.
j. CNSS NSS Instruction 1230 (ODNI/CIO Draft), Risk Management Guide for National Security Information Technology Systems, provides guidance on the assessment and mitigation of risk as part of an overall risk management process.
k. CNSS NSS Instruction 1237 (Draft), Guide for the Security Certification and Accreditation of National Security Information Systems, provides guidance on the security authorization of NSSs.

l. CNSS NSS Instruction No. 1253 (ODNI/CIO Draft), Security Control Catalog for National 9 Security Systems.
m. CNSS NSS Instruction 1253A (Draft), Guide for Assessing the Security Controls in National Security Information Systems, provides guidance for determining the effectiveness of security controls.
n. CNSS NSS Instruction 1260 (Draft), Security Categorization of National Security Information and Information Systems.
o. DCID 6/5, Policy for Protection of Certain Non-SCI Sources and Methods Information (SAMI).
p. DCID 6/9, Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs).
q. Department of Justice (DOJ) Order 2600.2C, Security Programs and Responsibilities.
r. DOJ Security Program Operating Manual (SPOM).
s. DOJ Order 2610.2A, Employment Security Regulations. Government Paperwork Elimination Act, 44 USC 3504.
t. DOJ Order 2880.1B, Information Resources Management.
u. DOJ Order 2740.1, Use and Monitoring of DOJ Computers and Computer Systems.
v. Federal Information Processing Standard (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules.
w. FIPS Publication 199, Standards for Security Categorization of Federal Information Systems.
x. FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
y. FIPS Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors.
z. Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements.
aa. Intelligence Community Directive Number 503, Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation.
bb. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook.
cc. NIST SP 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems.
dd. NIST SP 800-16, Information Technology Security Training Requirements.
ee. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
ff. NIST SP 800-27, Engineering Principles for Information Technology Security.
gg. NIST SP 800-28, Guidelines on Active Content and Mobile Code.
hh. NIST SP 800-30, Risk Management Guide for Information Technology Systems.
ii. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.
jj. NIST SP 800-35, Guide to Information Technology Security Services.
kk. NIST SP 800-36, Guide to Selecting Information Technology Security Products.
ll. NIST SP 800-37, Guide for the Security Certification and Accreditation for Federal Information Systems.
mm. NIST SP 800-39, Managing Risk from Information Systems.

nn. NIST SP 800-40, Creating a Patch and Vulnerability Management Program.
oo. NIST SP 800-41, Guidelines on Firewalls and Firewall Policy.
pp. NIST SP 800-44, Guidelines on Securing Public Web Servers.
qq. NIST SP 800-45, Guidelines on Electronic Mail Security
rr. NIST SP 800-46, Security for Telecommuting and Broadband Communications.
ss. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.
tt. NIST SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks.
uu. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.
vv. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations.
ww. NIST SP 800-53, Recommended Security Controls for Information Systems.
xx. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.
yy. NIST SP 800-54, Border Gateway Protocol Security.
zz. NIST SP 800-55, Security Metrics Guide for Information Technology Systems.
aaa. NIST SP 800-59, Guideline for Identifying an Information System as a National Security System.
bbb. NIST SP 800-60 (Vol. I and II), Guide for Mapping Type of Information and Information Systems to Security Categories.
ccc. NIST SP 800-61, Computer Security Incident Handling Guide
ddd. NIST SP 800-63, Electronic Authentication Guideline.
eee. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.
fff. NIST SP 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.
ggg. NIST SP 800-70, Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers.
hhh. NIST SP 800-76, Biometric Data Specification for Personal Identity Verification.
iii. NIST SP 800-77, Guide to IPsec VPNs.
jjj. NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide.
kkk. NIST SP 800-83, Guide to Malware Incident Prevention and Handling.
lll. NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.
mmm. NIST SP 800-88, Guidelines for Media Sanitization.
nnn. NIST SP 800-92, Guide to Computer Security Log Management.
ooo. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS).
ppp. NIST SP 800-95, Guide to Secure Web Services.
qqq. NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.
rrr. NIST SP 800-100, Information Security Handbook: A Guide for Mangers.
sss. NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices.
ttt. NIST SP 800-113, Guide to SSL VPNs.
uuu. NIST SP 800-114, User's Guide to Security External Devices for Telework and Remote Access.

vvv. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment.
www. NIST SP 800-121, Guide to Bluetooth Security.
xxx. NIST SP 800-123, Guide to General Server Security.
yyy. NIST SP 800-124, Guidelines on Cell Phone and PDA Security.
zzz. National Security Agency (NSA)/ Central Security Service (CSS) Policy 9-12, NSA/CSS Storage Device Declassification.
aaaa. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 1000, National Information Assurance C&A Process (NIACAP).
bbbb. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products.
cccc. National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95, RED/BLACK Installation Guidance.

3. Presidential and Office of Management and Budget Guidance

a. Executive Order 12958, Classified National Security Information, as amended.
b. EO 12968, Access to Classified Information.
c. EO 13231, Critical Infrastructure Protection in the Information Age.
d. EO 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans.
e. General Accounting Office (GAO) Federal Information System Control Audit Manual (FISCAM).
f. International Standard 15408, Common Criteria for Information Technology Security Evaluation.
g. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection,
h. HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors.
i. Memorandum for The Heads of Executive Departments and Agencies, Designation and Sharing of Controlled Unclassified Information (CUI).
j. National Security Directive 42, National Policy for the Security of National Security and Telecommunications and Information Systems.
k. National Security Presidential Directive (NSPD 51) / Homeland Security Presidential Directive (HSPD-20), National Continuity Policy.
l. Office of Management and Budget (OMB) Circular A-127, Financial Management Systems.
m. OMB Circular A-130, Management of Federal Information Resources (with Appendices and periodic revisions).
n. OMB Memorandum 99-18, Privacy Policy on Federal Web Sites.
o. OMB Memorandum 00-13, Privacy Policies and Data Collection on Federal Web Sites.
p. OMB Memorandum 01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy.
q. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.
r. OMB Memorandum 04-26, Personal Use Policies and "File Sharing" Technology.

s. OMB Memorandum 05-02, Financial Management Systems.
t. OMB Memorandum 06-15, Safeguarding Personally Identifiable Information.
u. OMB Memorandum 06-16, Protection of Sensitive Agency Information.
v. OMB Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.
w. OMB Memorandum 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.
x. OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
y. OMB Memorandum 07-18, Ensuring New Acquisitions Include Common Security Configurations.
z. OMB Memorandum 07-24, Updated Principles for Risk Analysis.
aa. OMB Memorandum 08-05, Implementation of Trusted Internet Connections (TIC).
bb. OMB Memorandum 08-16, Guidance for Trusted Internet Connection Statement of Capability Form (SOC).
cc. OMB Memorandum 08-22, Guidance on the Federal Desktop Core Configuration (FDCC).
dd. OMB Memorandum 08-23, Securing the Federal Government's Domain Name System Infrastructure.
ee. OMB Memorandum 08-27, Guidance for Trusted Internet Connection (TIC) Compliance.
ff. OMB Memorandum 09-02, Information Technology Management Structure and Governance Framework.

memory sticks are examples of devices that cannot be traded and must be replaced if defective.

e. The Contractor shall provide a written summary with a detailed explanation of what system or subsystem will be affected prior to any software or firmware being installed or any option changed in DEA's system. The summary shall provide an explanation of the risks to include impact of any subsystems and the expected benefit(s) to the Government of the new version of software/firmware or option. The summary shall include the estimated time required to install the software and what measures will be taken to minimize the impact while the installation is taking place. The summary must cover the Contractor's plan to restore or revert the system back to the previous status should the upgrade fail or produce unwanted results. The Contractor shall give the Government the option to perform the install during regular business hours or perform after 1:00 AM and ending before 8:00 AM to reduce operational impact at no additional cost to the Government.

f. The Contractor shall keep a stock of most replaceable items that generally fail to prevent a long lead time for part replacement.

g. The Contractor shall keep a log of complaints filed on the system performance. The log shall track and report the status of these complaints monthly to the Government. The log shall list all complaints that are open, all closed within the last 60 days, and those being researched by the Contractor. The log shall contain the nature of the complaint and when the complaint was reported; what subsystem was affected, and how and when the complaint was resolved. No complaint can be closed until the Government agrees to the closure of the complaint.

4. SECURITY

All contract personnel working on this contract shall have a Secret security clearance. Contractor personnel must have their security clearance granted through the Department of Defense (DOD) Defense Security Service (DSS). Only U.S. citizens, by birth or naturalized, shall be permitted to perform services under this contract. DEA will conduct record checks to supplement and update the DOD/DSS background investigation for all contractor personnel. The Office of Security Programs, Personnel Security Section (ISR) will conduct a suitability review of all contractor personnel. A final suitability determination will come from ISR on Contractors requiring access to DEA facilities, systems, or DEA Sensitive/National Security Information.

5. PLACE OF PERFORMANCE

The work will be performed at the Special Operations Division.

6. PERIOD OF PERFORMANCE

A contract will be awarded for a base period of one (1) year plus four (4) one-year option periods.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE	OMB Clearance Control Number:
	DJD-13-C-0016	1103-0018

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
0002	see block 16c	PR D-13-OS-0086	

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than item 6)	CODE
DEA Headquarters 8701 Morrissette Drive, Attn: (FACI/REBECCA STEGALL) Springfield, VA 22152	HQ		

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, state and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
VERINT TECHNOLOGY INC 330 SOUTH SERVICE ROAD MELVILLE, NY 11747-3257		9B. DATED (SEE ITEM 11)
	X	10A. MODIFICATION OF CONTRACT/ORDER NO. DJD-13-C-0016
		10B. DATED (SEE ITEM 13) 12/20/2012
CODE 541924753	FACILITY CODE 100549828	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

NA

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER (Specify type of modification and authority) Mutual Agreement of the Parties

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return ___1___ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this bilateral modification is to hereby incorporate the following clauses.

a) DEA-2852.203-70 FORMER EMPLOYMENT OR ASSIGNMENT WITH THE DEA (MAY 2013)
b) DEA-2852.231-70 OFFICIAL TRAVEL REQUIREMENTS (JUN 2013)
c) All other terms and conditions remain unchanged.

(see continuation page and attached replacement pages)

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Al Barresi - President	Taylor,Lisa
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED 7/23/2013
16B. UNITED STATES OF AMERICA By (Signature of Contracting Officer)	16C. DATE SIGNED 7-24-13

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA FAR (48 CFR) 53.243

Section 2 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN **Line Period of Performance:** 01/01/2013 - 12/31/2013	(b)(4)			
				PREVIOUS TOTAL	$1,447,294.80
				CHANGE	$0.00
				CURRENT TOTAL	$1,447,294.80

a) DEA-2852.203-70 FORMER EMPLOYMENT OR ASSIGNMENT WITH THE DEA (MAY 2013) is incorporated into the contract document in Full Text and replacement page is attached.
b) DEA-2852.231-70 OFFICIAL TRAVEL REQUIREMENTS (JUN 2013) is incorporated into the contract document in Full Text and replacement page is attached.

A vertical line in the right margin indicates changes. The contractor shall make complete page substitution in the contract as follows:

Section	Remove	Insert
3	Page 3-11	Page 3-11 thru 3-13

3.17 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

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

3.18 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

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

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **60** months from date of contract award.

(End of clause)

3.19 DEA-2852.203-70 FORMER EMPLOYMENT OR ASSIGNMENT WITH THE DEA (MAY 2013)

The contractor shall identify any contractor personnel who currently work for DEA, or have been employed with DEA within the last two years, or who will be working at, or providing support for, the same DEA Division or Office where they were last assigned prior to leaving DEA under the contract/task order. Any contractor personnel identified by the contractor must complete a Contractor Ethics Questionnaire. The contractor must provide this questionnaire to the contracting officer prior to the individual beginning performance on this effort. Depending on the responses provided, contractor personnel may be disqualified from the contract or required to seek a post-employment opinion from the DEA Office of Counsel to determine whether their work on, or support of, the contract/task order raises any conflict of interest issues or other potential violations of law.

The Contractor understands that contractor personnel are prohibited from appearing before, or communicating with, the Federal Government on behalf of a contractor regarding a Government contract, investigation or other particular matter that they participated in personally and substantially as a Federal employee with the intent to influence Government officials in those matters for the lifetime of those matters.

The Contractor further understands that for two years after leaving the Federal Government,

contractor personnel are prohibited from appearing before, or communicating with, the Government with the intent to influence on behalf of a contractor regarding a Government contract, investigation or other particular matter that they did not participate in personally and substantially as a Government employee, but that was under their official responsibility during their last year in the Government.

If DEA determines that after reviewing questionnaire responses or conducting other inquiries that contractor personnel may violate the above post-employment restrictions or other applicable laws if allowed to work on or support the contract/task order, at DEA's request, the contractor must remove those contractor personnel from the contract.

(End of clause)

3.20 DEA-2852.231-70 OFFICIAL TRAVEL REQUIREMENTS (JUN 2013)

In the performance of this contract, Contractor personnel may be required to conduct official travel. All travel costs will be authorized on a case-by-case basis and approved as set forth herein. All travel must be reviewed and pre-approved by the Contracting Officer's Representative (COR) prior to travel. Any expenses incurred by Contractor personnel without prior Government approval may be denied for payment. Authorization must be contingent on sufficient funds being available to cover the costs of travel. The Contractor will be reimbursed for actual, allowable travel costs and travel allowances (per diem), including transportation, lodging, meals and incidental expenses of personnel who are authorized to travel, in accordance with the established policy of Federal Acquisition Regulation (FAR) Part 31 and the Federal Travel Regulation (FTR). Furthermore, all travel arrangements shall be made under most prudent traveler (cost-effective) and efficient for the government criteria.

Travel expenses will be reimbursed on an actual expense basis. Travel expenses shall not include fees or overhead, unless specifically addressed elsewhere in this contract. No direct travel costs from place of residence to and from the normally assigned worksite will be allowable under this contract. The Contractor shall engage only the minimum number of travelers and vehicles needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible. Travel costs will not be reimbursed in an amount greater than the cost of and time required for coach class commercially scheduled air or ground travel by the most expeditious route. Exceptions to these limits must be addressed with the Contracting Officer.

Domestic U.S. travel rates (i.e., per diem, mileage, etc.) can be found on the General Services Administration (GSA) website (http://www.gsa.gov) under the "Travel Resources" section. Maximum rates of per diem allowance and reimbursements for miscellaneous travel expenses for travel in foreign areas, including the Trust Territory of the Pacific Islands, are established by the Department of State (DoS) (http://aoprals.state.gov). Maximum rates of per diem allowances and reimbursements for miscellaneous travel expenses for travel in Alaska, Hawaii, Puerto Rico, Northern Marianna Islands and territories and possessions of the United States are established by the Department of Defense (http://www.defensetravel.dod.mil/site/perdiem.cfm).

DOMESTIC TRAVEL

Contractors are authorized to use commercial air, commercial rail, rental vehicle, Government vehicle as a passenger, company authorized vehicle, or privately owned vehicle when travel is approved. When a mode other than commercial air is contemplated, the Contractor shall contact the COR to determine the mode of travel most advantageous to the Government. The Contractor will be reimbursed by the Government for actual air/rail fare and mileage incurred in direct support of the contract for travel specifically authorized by the COR or the Contracting Officer.

INTERNATIONAL TRAVEL

The Contractor shall be responsible for ensuring that all employees expecting to undertake international travel have a valid passport. DEA does not represent or guarantee a "US Official Government" passport will be issued by the Department of State.

International travel to specific countries and regions may be subject to additional Department of State requirements, as well as host nation requirements, such as visas. The Contractor shall be responsible for complying with any applicable DoS and destination national requirements and notifying the COR of any matters that impact cost, schedule, or performance.

TRAVEL INVOICE

The Contractor must submit a travel invoice upon the completion of travel. The travel invoice must be submitted to the COR with the monthly invoice following the completion of travel and contain all documentation, including receipts supporting the travel costs and evidence of DEA pre-authorization to travel. The documentation shall include the following information: traveler's name(s), purpose of travel, destination, Contract Number, Task Order Number (if applicable), Contract Line Item Number (CLIN), name of DEA official authorizing the travel, date of authorization and a breakdown of actual travel costs. The travel cost breakdown shall include per diem for the total number of travel days, lodging, miscellaneous and incidental expenses (including tolls, mileage, etc.), differential and allowances, with subtotals by category and a grand total. Vouchers and receipts shall be attached to invoices.

(End of clause)

[End of Section]

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE: DJD-13-C-0016	OMB Clearance Control Number: 1103-0018

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
0003	01/01/2014	See Lines	

6. ISSUED BY CODE	7. ADMINISTERED BY (If other than Item 6) CODE
HQ	

DEA Headquarters
8701 Morrissette Drive, Attn: (FACI/REBECCA STEGALL)
Springfield, VA 22152

8. NAME AND ADDRESS OF CONTRACTOR (No., street, country, state and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
VERINT TECHNOLOGY INC 330 SOUTH SERVICE ROAD MELVILLE, NY 11747-3257		9B. DATED (SEE ITEM 11)
	X	10A. MODIFICATION OF CONTRACT/ORDER NO.: DJD-13-C-0016
		10B. DATED (SEE ITEM 13): 12/20/2012
CODE 541924753	FACILITY CODE 100549828	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

2013-2013-S1R-OS-2560000-DOM-G2-01LK-ENF-25218-SOD-2560000

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER (Specify type of modification and authority) 52.217-9 Option to Extend the Term of the Contract

E. IMPORTANT: Contractor ☒ is not, ☐ is required to sign this document and return copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

a. The purpose of this modification is to exercise Option Period I in accordance with FAR Clause 52.217-9 Option to Extend the Term of the Contract. The period of performance is hereby changed from 01/01/2013 through 12/31/2013 to 01/01/2014 through 12/31/2014.

b. Option Period I is fully funded in the amount of (b)(4)

c. All other terms and conditions remain unchanged.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Taylor,Lisa	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA By (Signature of Contracting Officer)	16C. DATE SIGNED 12/11/2013

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA FAR (48 CFR) 53.243

Section 2 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN **Line Period of Performance:** 01/01/2013 - 12/31/2013	(b)(4)			
0002	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN **Line Period of Performance:** 01/01/2014 - 12/31/2014				
0003	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN **Line Period of Performance:** 01/01/2015 - 12/31/2015				
0004	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN **Line Period of Performance:** 01/01/2016 - 12/31/2016				
0005	ANNUAL TECHNICAL SUPPORT AND MAINTENANCE PLAN **Line Period of Performance:** 01/01/2017 - 12/31/2017				

PREVIOUS TOTAL	$1,447,294.80
CHANGE	$0.00
CURRENT TOTAL	$1,447,294.80

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	OBLIGATED AMOUNT	ACCOUNTING CODES
N/A	1	(b)(4)	2013 - S1R - OS 2560000 - DOM-G2 - 01LK - ENF - 25218 - - - SOD - - 2560000
N/A	2		2014 - S1R - OS - 2560000 - DOM-G2 - 01LK - ENF - 25218 - - - SOD - - - 2560000