OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC

John Greenewald, Jr.
27305 W. Live Oak Road
Suite #1203
Castaic, CA 91384

December 15, 2020

RE: ODNI MDR Tracking No. DEOM-2021-00001

Mr. Greenewald:

This letter responds to your Mandatory Declassification Review ("MDR") request dated 17 November 2020, received in the Office of the Director of National Intelligence ("ODNI") Information Management Office ("IMO") on 18 November 2020. Pursuant to Section 3.5 of Executive Order ("E.O.") 13526, you requested declassification review of *"Office of the Inspector General of the Intelligence Community Report Case Number 2013-0034, dated September 10, 2014."*

IMO located the previously reviewed and released version of the document responsive to your request. For your situational awareness, there are only 6 portions of the document that were withheld as classified in the FOIA review and release completed 29 December 2016. These portions are located on pages 2, 5, 6, 16, 27, and 32, and are marked with FOIA exemption (b)(1). IMO has determined that the portions of the document withheld pursuant to FOIA exemption (b)(1) remain currently and properly classified in accordance with Section 1.4(c) of E.O. 13526. Additionally, the same information in the document requires withholding pursuant to Section 3.5(c), under the following statute: The National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which protects intelligence sources and methods information. All remaining FOIA redactions were also reviewed and have been determined to be current and valid. We have provided a copy of the document for your use (Enclosure).

If you are not satisfied with IMO's response to your request, you may administratively appeal this decision by submitting a written request to the Director, Information Management Office, Office of the Director of National Intelligence, Washington, DC 20511 or DNI-FOIA@dni.gov. The request letter and envelope, or subject line of the email, should be marked "MDR Appeal." The appeal must specify the document(s) or information to be considered on appeal. Your appeal must be postmarked or electronically transmitted within 60 days of the date of this letter.

You may contact ODNI IMO's Requester Service Center at DNI-FOIA@dni.gov or (301) 243-1499 with any questions.

Sincerely,

Sally A. Nicholson

Sally A. Nicholson
Chief, Information Review &
Release Group
FOIA Public Liaison
Information Management Office

Enclosure

~~SECRET//NOFORN~~

OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY
INVESTIGATIONS DIVISION
WASHINGTON, DC 20511

REPORT OF INVESTIGATION

CASE NUMBER: 2013-0034 **SEP 10, 2014**

SUBJECT

(U//~~FOUO~~) [redacted] (AIN [redacted] b3 b6 b7C - IG Subject

ALLEGATIONS

1. (U//~~FOUO~~) Subject engaged in conflicts of interest.

2. (U//~~FOUO~~) Subject engaged in improper or unauthorized outside employment.

3. (U//~~FOUO~~) Subject engaged in falsification and misrepresentation.

4. (U//~~FOUO~~) Subject misused government information and information systems.

5. (U//~~FOUO~~) Subject engaged in sexual misconduct while on duty.

Classified By: [redacted] - IC IG b3 b6
Derived From: ODNI MET S-12
Declassify On: 25X1, 20641231

~~SECRET//NOFORN~~

BACKGROUND

~~(S//NF)~~ On August 23, 2012, the Clearance Division of the CIA Office of Security contacted the Special Investigations Branch (SIB) regarding [redacted] (AIN [redacted]), a Senior Security Database Program Officer for the Office of the Director of National Intelligence National Counterintelligence Executive (NCIX). During a re-adjudication investigation for [redacted] the Clearance Division found evidence that [redacted] engaged in unreported outside activities. As part of the standard operating procedure for the Clearance Division, the matter was referred to SIB.

b3
b6
b7C - IG Subject

~~(S//NF)~~ During the SIB investigation, case reviewers discovered that [redacted] had two unreported part-time facility security officer (FSO) consulting contracts, in addition to five part-time FSO consulting contracts she had reported. Based on that discovery, SIB audited her computer use to determine if she was engaged in personal business during duty hours.

b3
b6
b7C - IG Subject

~~(S//NF)~~ SIB discovered AIN evidence that [redacted] had part-time FSO business relationships with approximately 14 companies. SIB also discovered archived time and attendance sheets for work performed for these companies and documentation noting her FSO relationship to those companies. [redacted] revealed that [redacted] averaged in excess of five hours per day on personal affairs and unofficial business.

b1
b3
b6
b7C - IG Subject

~~(S//NF)~~ Based on information and belief, SIB suspected that [redacted] used her security officer privileges to query whether SIB was investigating her.

b3
b6
b7C - IG Subject

(U//~~FOUO~~) [redacted]

b3
b6
b7C - IG Subject

(U//~~FOUO~~) [redacted]

b3
b6
b7C - IG Subject

(U//~~FOUO~~) [redacted] b3 b6 b7C - IG Subject

(U//~~FOUO~~) [redacted] b3 b6 b7C - IG Subject

(U//~~FOUO~~) [redacted] b3 b6 b7C - IG Subject

SCOPE

(U//~~FOUO~~) The Investigations Division (INV) of IC IG conducted this investigation pursuant to 50 USC § 3033, Inspector General of the Intelligence Community, effective 7 October 2010; ODNI Instruction 10.34, Office of the Inspector General of the Intelligence Community, dated 22 Sept 2013; and, the Quality Standards for Investigations, dated 15 November 2011, set forth by the Council of the Inspectors General on Integrity and Efficiency.

ALLEGATION 1

(U//~~FOUO~~) Subject engaged in a conflict of interest.

APPLICABLE LAW AND POLICY

(U) Compensation to Members of Congress, officers, and others in matters affecting the Government. Title 18, United States Code, Section 203 provides that, with certain exceptions, "whoever...directly or indirectly demands, seeks, receives, accepts, or agrees to receive or accept any compensation for any representational services, as agent or attorney or otherwise, rendered or to be rendered either personally or by another at a time when such person is an officer or employee...of the United States in the executive...branch of the Government...in relation to any proceeding, application, request for a ruling or other determination, contract, claim, controversy, charge, accusation, arrest, or other particular matter in which the United States is a party or has a direct and substantial interest, before any department..." is guilty of a federal offense.

(U) Activities of officers and employees in claims against and other matters affecting the Government. Title 18, United States Code, Section 205 provides that, with certain exceptions, "whoever, being an officer or employee of the executive branch of the United States Government... acts as agent or attorney for anyone before any department, agency, court, court-martial, officer, or civil, military, or naval commission in connection with any covered mater in which the United States is a party or has a direct interest" is guilty of a federal offense.

(U) Use of Nonpublic Information. 5 C.F.R. § 2635.703 provides that "an employee shall not engage in a financial transaction using nonpublic information, nor allow the improper use of nonpublic information to further his own private interest or that of another, whether through advice or recommendation, or by knowing unauthorized disclosure."

ANALYSIS

(U//~~FOUO~~) began her tenure at the ODNI on May 10, 2010. She entered the ODNI as a GS-14 in the role of Senior Security Database Program Officer at the Office of the National Counterintelligence Executive (NCIX). In her role as a program officer, is expected to "manage...the Scattered Castles repository, , and the Sensitive Compartmented Information Facility (SCIF) Database."[1] Her role also requires her to "monitor the Security Databases Program budget and author and compile well-reasoned budget planning and execution recommendations to the Security Databases Program Manager."[2] role at the ODNI allows her unfettered access to Scattered Castles, JPAS, and a host of other security related databases and sites. According to due to her role at the ODNI, she has the ability to change information within these security databases to include resolving redundancies, changing dates, or changing access for those with security clearances.[3]

b3
b6
b7C - IG Subject

(U//~~FOUO~~) According to and Standard Form 86 (SF86), she has also worked as a Facility Security Officer since December 2007 for several companies. A Facility Security Officer (FSO) administers and assures compliance with security regulations and procedures in accordance with a

b3
b6
b7C - IG Subject

---

[1] ODNI Vacancy Notices, *ODNI/DNI Security Databases Program Officer 20747,* Personnel File, 19 August 2009.
[2] Ibid.
[3] *personal interview with IC IG,* 30 July 2014.

b3
b6
b7C - IG Subject

contract's guidelines. They serve as the point of contact for contractor security matters and are familiar with all aspects of security including personnel, physical, operations, industrial, communications, information, and information technology security. An FSO directs and advises all departments regarding security regulations and procedures, and routinely interacts with Government agencies relative to security matters.[4] FSOs are considered Key Management Personnel (KMP), and must be at least part-time employees in order for a contractor to properly maintain a facility's security. According to [redacted] and an audit of her US Government system, one of the primary functions of her job as an FSO, is working within security databases and providing assistance to employees regarding their clearance paperwork and processing.

b3
b6
b7C - IG Subject

(U~~//FOUO~~) On April 29, 2013, the IC IG opened a preliminary inquiry into [redacted] upon receiving a referral from CIA OIG and SIB due to the subject's failure to adhere to [redacted] and any subsequent laws or policies. The initial information included in the referral regarded unreported outside activities. As standard procedure, [redacted] (EXHIBIT M)

b3
b6
b7C - IG Subject
b7E - IG Tech

(U~~//FOUO~~) The [redacted] over 856 files pertaining to outside activities, including classified contracts (DD254s); time and attendance records; SF86s for employees; JPAS documents; offer letters; and invoices. In total, there was 337.54 MB[5] of outside activity related documents on [redacted] AIN account.

b3
b6
b7C - IG Subject
b7E - IG Tech

(U~~//FOUO~~) The [redacted] web activity associated with FSO work, and the maintenance of over 600 files on a US Government system pertaining to FSO work.[6] [redacted], the IC IG found several instances where [redacted] accessed JPAS from a US Government system while on duty as a federal employee for the purposes of FSO related activity.[7] Furthermore, the [redacted] multiple instances of communication between government

b1
b3
b6
b7C - IG Subject
b7E - IG Tech

[4] Derived from vacancy notices at different government contractor websites and the Department of Security Services website.

[5] 337.538MB is 1/3 of a GB, or the complete works of Shakespeare, 100 times.

[6] Although outside the scope of the investigation, it should be noted that [redacted] engaged in sexually explicit [redacted] with a contractor for the first year of working at ODNI. Please see [redacted]

b3
b6
b7C - IG Subject

[7] Improper maintenance of PII and improper use of government systems is discussed in the following allegations.

agencies and [redacted] in her role as an FSO on a US Government system during duty hours. Specifically, the [redacted] communication between [redacted] in her role as FSO representing a company back to the federal government through DSS as the point of contact for the company while on duty as a federal employee. (EXHIBIT AA, DD)

b3
b6
b7C - IG Subject
b7E - IG Tech

(U~~//FOUO~~) During the investigation, [redacted] continued to act as key management personnel for the companies, and continued working on these activities while on US Government systems during duty hours.

b3
b6
b7C - IG Subject

(U~~//FOUO~~) In or around May 3, 2013, [redacted] second line supervisor overheard [redacted] negotiating terms of a contract on the phone while at work.[8] The second line supervisor was told by [redacted] first line supervisor that she maintained outside activities. Out of concern regarding 18 USC § 205, the second line supervisor asked [redacted] for a list of the companies she represented and her duties for each company. [redacted] provided a list of the companies (EXHIBIT CCCC, DDDD):

b3
b6
b7C - IG Subject

Company	**Start Date**	**Title**
Wheeler Network Design	December 2007	FSO
Link Solutions Inc	October 2007	FSO
Twin Soft Corp	May 2009	FSO
IncaTech	April 2010	FSO
Geographic Services Inc	October 2010	"not FSO"
C5i Federal	May 2012	FSO
GuROO IT	July 2012	FSO
Technology Science Corporation	November 2012	FSO

[8] Date was derived [redacted] an email dated May 9, 2013 to [redacted], in where she tells [redacted] she met with [redacted] "on Friday."

b1
b3
b6
b7C - IG Subject, Witnesses
b7E - IG Tech

Maverick LLC	November 2012	FSO
FS-ISAC	January 2013	FSO
Augusta Westland	2008	"not FSO"

(U//~~FOUO~~) The second line supervisor met with [redacted] and went over the company list, duties, as well as looked at her 879s. [redacted] told the second line supervisor that she was told "just don't list you're an FSO and you'll be fine" by OGC, and that is why her 879s were vague. The supervisor found this to be unbelievable and asked that [redacted] put a hold on all outside activities until it was resolved. He also alerted Office of Security and OGC to his concerns.

b3
b6
b7C - IG Subject

(U//~~FOUO~~) In an email dated May 8, 2013, the second line supervisor wrote to the Office of Security, "[redacted] was notified of an approval for outside activities today, the problem is no one in her supervisory line approved the outside activity. The outside employment is very questionable regarding conflict of interest and we are still collecting information regarding [redacted] relationship and exact duties with these companies...I am requesting that you withdraw your approval of Ms. [redacted] outside activities until you receive an approval from her supervisor." (EXHIBIT CCCC, DDDD)

b3
b6
b7C - IG Subject

(U//~~FOUO~~) On May 8, 2013, the Office of Security responded, "We will add a note to Ms. [redacted] 879 request noting that it is in pending status while we wait for more information from you."

b3
b6
b7C - IG Subject

(U//~~FOUO~~) After the initial confrontation with [redacted] her second line supervisor maintained that there were conflicts of interest. On August 14, 2013, the IC IG interviewed the supervisor. He stated that after meeting with [redacted] in May, and asking more questions regarding her outside activities, he felt that her FSO duties were clearly in conflict with her role as a government employee. He described [redacted] as "problematic:" [redacted] received counseling on several issues including time and attendance issues and poor leave time management.

b3
b6
b7C - IG Subject

(U//~~FOUO~~) On August 15, 2013, the supervisor wrote an email to the IC IG investigator stating, "[redacted] first line supervisor] and I informed [redacted]

b3
b6
b7C - IG Subject

[redacted] that I have decided to non-concur on her request for outside employment for all ten firms. I cited my reasons as conflict of interest and my opinion of her not adhering to OGC guidance on representing a third party back to the government. When [her first line supervisor] attempted to reply to the outside activities request we found it had once again been approved without our approval. I asked the outside activities branch to reactivate the request so we can record our decision." b3 b6 b7C - IG Subject

(U//~~FOUO~~) On August 19, 2013, the IC IG spoke with the Deputy Director of the Special Security Directorate. She emailed the investigators to alert them to a meeting she was scheduled to have with [redacted] [redacted] requested the meeting to appeal the non-concur by second line supervisor. After the meeting, the Deputy Director wrote again to update the investigators: b3 b6 b7C - IG Subject

> "The decision hasn't changed, but there have been complications. Unfortunately, the Outside Activities reporting system had generated an automatic concurrence for [redacted] at some point in May after it got no input from the designated supervisor after a certain amount of time (I believe 5 days) (this is actually the second time this has happened). Last week, [redacted] second line supervisor] reached out to the office responsible for the system and told them he wished to non-concur as the supervisor, and they said [redacted] would have to generate another Outside Activities report, and resend it through the process. They also instructed [redacted] she had to do this. [He] still intends to non-concur (actually he is directing [the first line supervisor] as her supervisor to non-concur) and he has told [redacted] that. b3 b6 b7C - IG Subject
>
> When [redacted] met with me today she was looking for some way to appeal [the] decision. She said there was an appeal process for when OGC non-concurs, but nothing in the regs re when the supervisor non-concurs. She said she has spoken to the Ombudsman because she thinks [he] is being biased against her and she said they told her this might need to be an issue she needs to resolve with HR involvement. We ultimately decided: 1) she would send me the documentation on her outside employments that she's provided to [her supervisor]; 2) [The supervisor] would send his written concerns to her and me (justification for his non-concur); 3) I would send both of the above to the OGC rep who concurred on the Outside Activity report (since the nature of [his] concerns have to do with conflict of interest); 4) I would set up a meeting with me, [the supervisor], [redacted] and OGC b3 b6 b7C - IG Subject

to discuss the concerns. Out of that meeting, either [he] would still have his concerns and OGC could give [redacted] clarification/guidance, or OGC will explain to [him] why his concerns don't apply and [he] will likely be comfortable concurring. And finally 5) regardless of the outcome of the meeting, [redacted] would generate another Outside Report listing all of her outside employments and then OGC and [he] would chop on it documenting their final concurrence or non-concurrence for the record." (EXHIBIT VV)

b3
b6
b7C - IG Subject

(U//~~FOUO~~) On August 20, 2013, the IC IG spoke with OGC concerning the upcoming meeting with [redacted] and her supervisors. In the call, OGC explained to the IC IG that OGC would not be meeting with [redacted] as the decision was at the management level. If management did not concur, then the 879 would be non-concurred on and never be received or reviewed by OGC, [redacted]

b3
b6
b7C - IG Subject

(U//~~FOUO~~) By August 20, 2013, [redacted] had been admonished by OGC to maintain strict distance from outside activities that would have conflicts of interest, had been told by her first and second line supervisor to cease all outside activities, and had been told by OGC that the matter was not for appeal, and that [redacted] was to oblige her management's decisions.

b3
b6
b7C - IG Subject

(U//~~FOUO~~) On July 30, 2014, the IC IG interviewed [redacted] In the interview, [redacted]

b3
b6
b7C - IG Subject

(U//~~FOUO~~) [redacted]

b3
b6
b7C - IG Subject

CONCLUSION

(U//~~FOUO~~) [redacted]

b3
b6
b7C - IG Subject

ALLEGATION 2

(U//~~FOUO~~) Subject engaged in improper or unauthorized outside employment.

APPLICABLE LAW AND POLICY

(U) Acts Affecting a Personal Financial Interest. Title 18, United States Code, Section 208 provides that, "except as permitted by subsection (b) hereof, whoever, being an officer or employee of the executive branch of the United States Government...participates personally and substantially as a Government officer or employee, through decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise, in a judicial or other proceeding, application, request for a ruling or other determination, contract, claim, controversy, charge, accusation, arrest, or other particular matter in which, to his knowledge, he, his spouse, minor child, general partner, organization in which he is serving as officer, director, trustee, general partner or employee, or any person or organization with whom he is negotiating or has any arrangement concerning prospective employment, has a financial interest" is guilty of a federal offense.

(U) Salary of Government Officials and Employees payable only by United States. Title 18, United States Code, Section 209 provides that, "whoever receives any salary, or any contribution to or supplementation of salary, as compensation for his services as an officer or employee of the executive branch of the United States Government, of any independent agency of the United States, or of the District of Columbia, from any source other than the Government of the United States, except as may be contributed out of the treasury of any State, county, or municipality" is guilty of a federal offense."

(U) *Use of Nonpublic Information.* 5 C.F.R. § 2635.703 provides that "an employee shall not engage in a financial transaction using nonpublic information, nor allow the improper use of nonpublic information to further his own private interest or that of another, whether through advice or recommendation, or by knowing unauthorized disclosure."

ANALYSIS

(U//~~FOUO~~) Form 879 Outside Activities Form ("879") is required to be submitted by any member of the ODNI under [redacted] b3

[redacted] b3 The policy is in place to ensure, among other things, no conflicts of interest exist between the federal employee and the outside activity.

(U~~//FOUO~~) Furthermore, as stated [redacted] b3

(U) [redacted] No further information is sought; thus, the information on the 879 is the sole source in the determination.

(U~~//FOUO~~) On May 12, 2010, two days after joining the ODNI, [redacted] submitted an 879 to OGC/ELD for approval regarding work as a Facility Security Officer for four companies: Link Solutions, Inc; Wheeler Network Design; Twin Soft Corporation; and IncaTech LLC. She wrote, "I work for four small US Government contractors in my free time. ...They do not have any contracts with the IC. I am paid a minimal amount by them." On May 20, 2010, ten days after joining ODNI, [redacted] submitted a second 879 for approval regarding work as a Facility Security Officer for Augusta Westland North America. In the second 879, [redacted] wrote, "I am requesting approval prior to consulting for Augusta Westland North America...I would be doing purely administrative work for them...I would do this work after my regular scheduled duty hours with ODNI." (EXHIBIT CCCC, DDDD) b3 b6 b7C - IG Subject

(U~~//FOUO~~) Form 879 is automatically approved by a supervisor, should the request for approval remain in the supervisor's email inbox, unread, for five days. After five days, the form is automatically approved and sent to OGC/ELD. According to [redacted] first and second line supervisors, the b3 b6 b7C - IG Subject

request for outside activities by [redacted] was automatically approved and sent to OGC/ELD. b3 b6 b7C - IG Subject

(U~~//FOUO~~) On May 24, 2010, and June 4, 2010, respectively, the 879s submitted by [redacted] were concurred by OGC/ELD. The notification that an outside activities form has been approved includes several admonishments from OGC/ELD regarding 18 USC § 205 and CFR 2635. Among the admonishments, OGC/ELD advises, "Restriction on representation of private interest before the USG Executive branch employees are subject to criminal statutes that prohibit the representation of private interest before the Government. One of these laws prohibits an employee from acting as the agent or attorney of a private party before the government in connection with a particular matter in which the United States is a party of has a direct and substantial interest. See 18 USC 205." The guidance continues to specifically state, "The type of representation that is prohibited would include any personal appearance or communication to any federal agency on behalf of any of the four companies. For example, you could not sign documents or letters to be sent to any federal agency (not just ODNI) on behalf of any of the companies." [redacted] was also told that "an employee shall not allow the improper use of nonpublic information to further his own private interest." b3 b6 b7C - IG Subject

(U~~//FOUO~~) On April 24, 2013, [redacted] submitted a third 879 stating, "I work for 10 small US Government contractors in my free time. I provide them personnel security support (initiating, and submitting their clearance, fingerprinting their personnel for clearances and any general security questions/concerns). They all hold Secret & Top Secret facility clearances, issued by Department of Defense. None have foreign employees or foreign contracts. They do work for Department of State, WHCA, DHS, Army and DoD. They do not have any contracts with any agencies in the IC. They are: Link Solutions, Inc, employed since October 2007. Wheeler Network Design, employed since Dec 2007. Twin-Soft Corporation employed since May 2009. Incatech, one-woman company, employed since April 2010. Geographic Services, Inc, employed since October 2010. C5i Federal, employed since May 2012, GuROO IT, employed since July 2012, Maverick LLC, employed since November 2012 and Financial Services-ISAC, employed since Jan 2013." b3 b6 b7C - IG Subject

(U~~//FOUO~~) The form asks a series of prompts. One prompt asks "Indicate if you will be required to interact verbally or in writing with any federal government agency/department; please explain." [redacted] wrote, "During my b3 b6 b7C - IG Subject

own time, I send Visit Requests and Visit Authorization Letters using my personal email to government agencies for the company contractors to visit their facilities." At the bottom of the page, the form states "I understand I must report any changes to this particular Outside Employment activity" to which [redacted] responded, "Yes." OGC/ELD sought clarification on this particular answer from [redacted]. The OGC/ELD representative dealing with [redacted] 879 asked, "When you refer to DoD contracting agencies, do you mean other DoD contractors or DoD agencies?" to which [redacted] responded, "I mean other DoD contractors such as Lockheed Martin, Northrup Grumman and SAIC."

b3
b6
b7C - IG Subject

(U~~//FOUO~~) Between [redacted] EOD and March 11, 2013, the IC IG found [redacted] of communication between DoD agencies and [redacted] while she was on US Government systems during duty hours, and zero emails between [redacted] and Lockheed Martin, SAIC, or Northrup Grumman. (EXHIBIT M)

b3
b6
b7C - IG Subject
b7E - IG Tech

(U~~//FOUO~~) [redacted] On one occasion, [redacted] used Scattered Castles for her duties as an FSO: On September 6, 2013, [redacted] wrote to one company she represents, "JPAS still shows the 2007 investigation. In Scatter Castles, the FBI shows the 2013." On the same day, [redacted] communicated with a DSS official while on duty at ODNI and provided him with her contact information so that they could further discuss the facility clearance for a company. (EXHIBIT N)

b3
b6
b7C - IG Subject
b7E - IG Tech

(U~~//FOUO~~) On November 20, 2013, DCIS and IC IG [redacted] of [redacted] personal email. The [redacted] revealed over six gigabytes of information, including communication between [redacted] and fourteen companies.[9],[10] In one email dated October 2, 2013, [redacted] wrote

b3
b6
b7C - IG Subject
b7E - IG Tech

[9] C5i Federal; AWNA; Maverick LLC; Twin Soft Corporation; IncaTech LLC; Link Solutions Inc; GuROO IT; FS-ISAC; Electromagnetic Systems; GSI; Wheeler Network; Technology Science Corporation; Red Arch Solutions; Century Link.

[10] The list of fourteen companies is non-exhaustive. Several times in the emails reviewed, [redacted] referred to her "work email" in regards to different companies. The personal email

b3
b6
b7C - IG Subject

an email to contractors with the subject header "Leave (a furloughed vacation I suppose):" "Good morning everyone, I am writing to let you know next Tuesday, Oct 8 through Monday, October 14 I will not have access to JPAS. However, I will have access to email and regular internet connectivity." The email indicates that [redacted] was unable to perform her duties as an FSO while on furlough.

b3
b6
b7C - IG Subject

(U//~~FOUO~~) On January 8, 2014, the IC IG and DCIS requested [redacted] Several tax documents were sent by the companies [redacted] represents over the 30 day period. However, some companies did not send tax documentation, raising suspicion in regard to tax fraud.

b3
b6
b7C - IG Subject
b7E - IG Tech

(U//~~FOUO~~) The [redacted] as well as a review of the search warrant revealed several instances where she referred to her LinkedIn account and used it to solicit new work. On March 4, 2014, DCIS, IRS, and IC IG executed a search warrant on [redacted] LinkedIn account. The LinkedIn account search warrant results confirmed the use of LinkedIn as a means to garner business, and confirmed [redacted] connections to some of the key management personnel at the companies.

b3
b6
b7C - IG Subject
b7E - IG Tech

(U//~~FOUO~~) After the IRS joined the investigation, on March 11, 2014, DCIS, IRS, and IC IG [redacted]

b3
b6
b7C - IG Subject
b7E - IG Tech

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

---

communications indicated that [redacted] would use the account when her company email was unavailable

[11] [redacted] is a law enforcement investigative technique in which [redacted]

b3
b6
b7C - IG Subject
b7E - IG Tech

e. [redacted]

f. [redacted]

g. [redacted]

h. [redacted]

i. [redacted]

j. [redacted]

k. [redacted]

l. [redacted]

m. [redacted]

b3
b6
b7C - IG Subject
b7E - IG Tech

(U~~//FOUO~~) In total, [redacted] (counting only full, 365 day years that she has been employed by ODNI, and falsely reported outside activities), [redacted].

b3
b6
b7C - IG Subject
b7E - IG Tech

(U~~//FOUO~~) From March 5, 2014 to March 25, 2014, [redacted] (EXHIBIT WWW, XXX, YYY):

b3
b6
b7C - IG Subject
b7E - IG Tech

a. March 5, 2014 – An envelope addressed to [redacted] at [redacted], from 99999 Consulting LLC, 7032 Lee Mills Court, Springfield, VA. A pay stub was found in the opened envelope. The pay stub listed [redacted] and her Employee ID as 4. The pay period was listed as February 1, 2014 to February 15, 2014 and a check date of February 14, 2014. Gross pay on the pay stub was $400.00 and a net pay of $367.95. Year to date earnings as $367.95;

b3
b6
b7C - IG Subject

b. March 25, 2014 - An envelope addressed to [redacted] at [redacted], from Maverick Cyber

b3
b6
b7C - IG Subject

[12] A [redacted] is an undercover investigative technique. [redacted]. Law enforcement officers [redacted]

b7E - IG Tech

– Defense, 1400 C Street, Germain Drive, Centerville, VA 20121, postmarked March 19, 2014;

c. March 25, 2014 - An Earnings Statement from Maverick – Security LLC, 14408 Chantilly Crossing Lane, Chantilly, Virginia 20151, for [redacted] at [redacted], pay date March 11, 2014. Earnings for the pay period are $276.05 with a year to date earning of $600.00; b3 b6 b7C - IG Subject

d. March 25, 2014 - An envelope addressed to [redacted] at [redacted], from Link Solutions, Inc. 12007 Sunrise Valley Drive, Reston, VA 20191, postmarked December 16, 2013. b3 b6 b7C - IG Subject

~~(S//NF)~~ On March 14, 2014, the IC IG compiled a list of the companies represented by [redacted] that have Intelligence Community contracts. Despite [redacted] claims that none of the companies she represented worked for the Intelligence Community, a number of companies she represented held IC contracts. For example, Maverick LLC maintained contracts with ODNI and Defense Intelligence Agency (DIA); [redacted] maintained contracts with [redacted] and [redacted] FS-ISAC maintained contracts with DHS and ODNI; and [redacted]. maintained contracts with [redacted][13] (EXHIBIT WW, XX) b3 b6 b7C - IG Subject

(U~~//FOUO~~) Between March 2014 and May 2014, [redacted] revealed continued misuse of US Government systems through AIN and CWE, continued misuse of nonpublic information through JPAS and Scattered Castles, and continued false statements through time and attendance verifications and written statements to her supervisors regarding her outside activities. For example, on March 25, 2014, [redacted] used her US Government system while on duty at ODNI to agree, clarify, and help write the security portion of a bid for a DIA proposal for Technology Science Corporation. (EXHIBIT KK, LL) b3 b6 b7C - IG Subject b7E - IG Tech

(U~~//FOUO~~) On June 9, 2014, the IC IG received access to contract databases that would allow for a wider breadth of information pertaining to PURYEAR. It was discovered [redacted], that [redacted] is listed in government databases as key management personnel for GuROO IT LLC; b3 b6 b7C - IG Subject b7E - IG Tech

[13] Information for [redacted] and [redacted] gathered from [redacted]; all other contract data gathered from [redacted] b1 b3 b7E - IG Tech

Augusta Westland; Wheeler Network Design; INCATech LLC; FS-ISAC; Link Solutions; iKare Corporation; and Twin-Soft Corporation.

(U//~~FOUO~~) On July 30, 2014, the IC IG interviewed [redacted] In the interview, [redacted];[14]

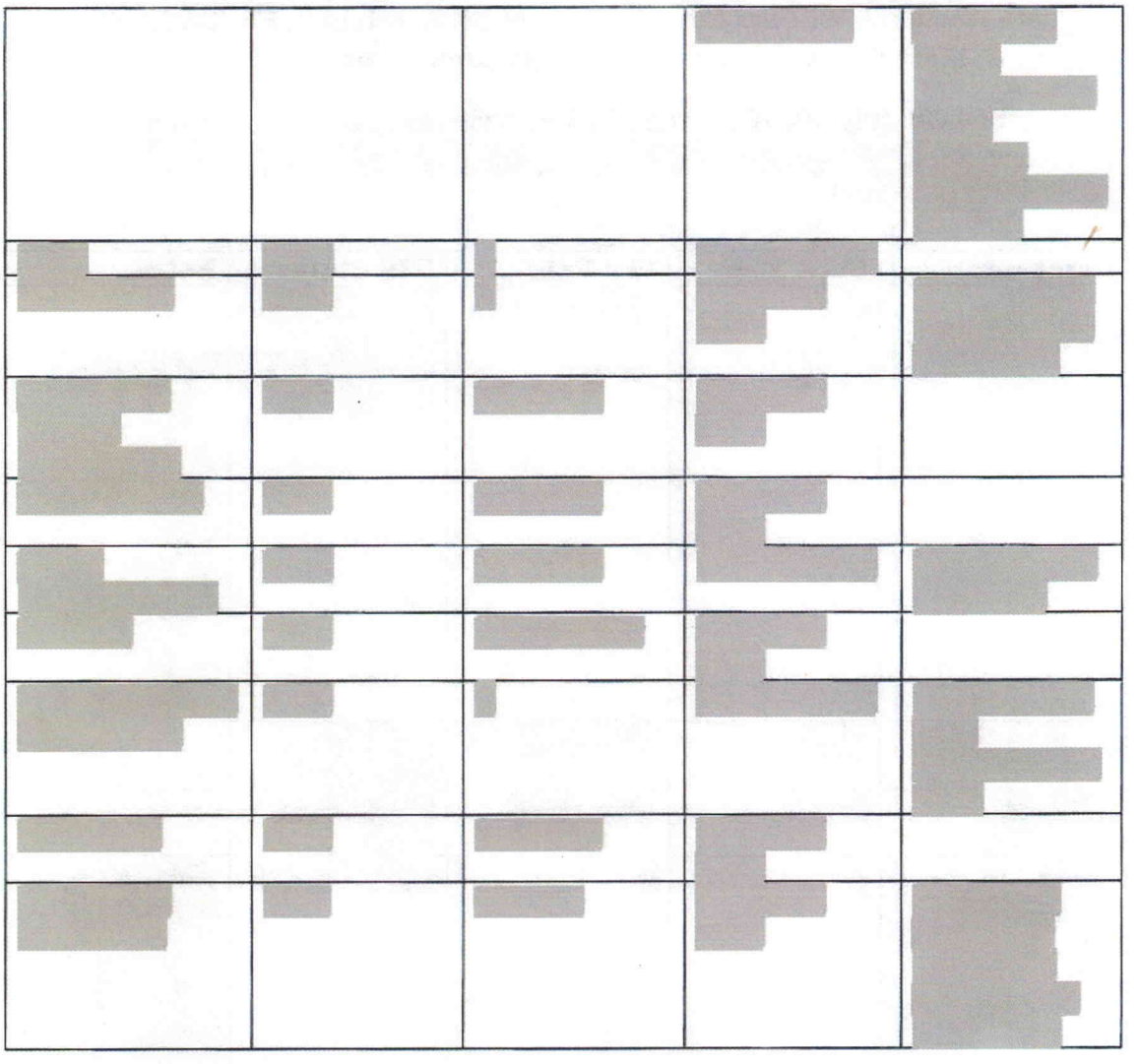
b3
b6
b7C - IG Subject

Company	Start Year	Pay Rate	879 Status	Notes
[redacted]				
[redacted]				
[redacted]				
[redacted]				

b3
b6
b7C - IG Subject

[14] [redacted]

b3
b6
b7C - IG Subject



b3
b6
b7C - IG Subject

(U//~~FOUO~~)

b3
b6
b7C - IG Subject

(U//~~FOUO~~)

b3
b6
b7C - IG Subject

(U//~~FOUO~~) [redacted] explained that she felt her second line supervisor was singling her out, although she could not explain why. She cited his checking of her time and attendance as evidence of his bullying and categorically denied any time and attendance fraud when it came to her physical presence.[15]

b3
b6
b7C - IG Subject

(U//~~FOUO~~) When asked about time and attendance fraud and dual compensation in regard to working on FSO duties and game playing while at ODNI, [redacted] said she understood that by recording her time and attendance as nine hours, when she spent at least four of those nine working on FSO duties, she was committing time and attendance fraud. [redacted]

b3
b6
b7C - IG Subject

CONCLUSION

(U//~~FOUO~~) [redacted]

b3
b6
b7C - IG Subject

ALLEGATION 3

(U//~~FOUO~~) Subject engaged in falsification and misrepresentation.

APPLICABLE LAW AND POLICY

(U) False Statements. Title 18, United States Code, Section 1001 provides that, with certain exceptions, "whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry" shall be guilty of a federal offense.

---

[15] [redacted] show 754.98 questionable hours indicating that the second line supervisor was acting well within reason to inquire after her time and attendance. (EXHIBIT K)

b3
b6
b7C - IG Subject
b7E - IG Tech

ANALYSIS

(U//~~FOUO~~) Between November 2013 and February 2014, [redacted] continued a pattern and practice of working on FSO duties while on duty at the ODNI. During this time period, [redacted] filed her taxes. The [redacted] revealed suspicious tax practices witnessed by investigators, as she filed her taxes at the ODNI using US Government systems.

b3
b6
b7C - IG Subject
b7E - IG Tech

(U//~~FOUO~~) [redacted] [16] [redacted]

b3
b6
b7C - IG Subject
b7E - IG Tech

(~~C//OC//LES-NF~~) [redacted] [17] [redacted]

b3
b6
b7C - IG Subject
b7E - IG Tech

---

[16] [redacted]

b3
b6
b7C - IG Subject

[17] [redacted]

[redacted] [18] b3 b6 b7C - IG Subject

(U//~~FOUO~~) On July 30, 2014, the IC IG interviewed [redacted] During the interview, [redacted] b3 b6 b7C - IG Subject

(U//~~FOUO~~) [redacted] For example, on May 9, 2013, [redacted] emailed a coworker to discuss her meeting with second line supervisor regarding her outside activities. She explicitly states that she was working to allay his concerns by being vague. When talking about the list of companies she provided to him she wrote, "I was vague and am pretty sure I didn't include everything he asked for. LOL this was Friday." (EXHIBIT PP) b3 b6 b7C - IG Subject

(U//~~FOUO~~) [redacted] b3 b6 b7C - IG Subject

CONCLUSION

(U//~~FOUO~~) [redacted] b3 b6 b7C - IG Subject

ALLEGATION 4

(U//~~FOUO~~) Subject misused government information and information systems.

---

[18] [redacted] b3 b6 b7C - IG Subject

APPLICABLE LAW AND POLICY

(U) Computer fraud. Title 18, United States Code, Section 1030(a)(2)(B) provides that whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains... information from any department or agency of the United States" is guilty of a federal offense.

(U) Privacy Act Violations. Title 5, United States Code, Section 552a(i)(2) provides that, "any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section" is guilty of a misdemeanor and shall be fined not more than $5,000.

(U) Use of Nonpublic Information. 5 C.F.R. § 2635.703 provides that "an employee shall not engage in a financial transaction using nonpublic information, nor allow the improper use of nonpublic information to further his own private interest or that of another, whether through advice or recommendation, or by knowing unauthorized disclosure."

(U) Access to Personnel Security Information. [redacted] provides that, "Agency personnel authorized to handle OS personnel security information as part of their official duties are expected to review the information only on a definite "need-to-know" bases as determined by the D/OS or designees. It is incumbent upon Agency personnel having access to personnel security information to preserve the confidential character of this information in accordance with the terms of this regulation and applicable law." b3

(U) Limited Use of Government Office Equipment Including Information Technology. [redacted] provides that "[redacted] Agency personnel are permitted limited use of government office equipment for personal needs if the use does not interfere with official business, involves minimal additional expense to the US Government, [redacted]." b3

ANALYSIS

(U//~~FOUO~~) [redacted] b7E - IG Tech

[redacted] from May 23, 2013 to May 23, 2014. In that time period there were 12,121 instances of JPAS use. (EXHIBIT X) [redacted] approximately 59% of [redacted] JPAS use was performed while at the ODNI on US Government systems.[19] [redacted] pattern and practice of misusing the nonpublic information in JPAS by accessing JPAS records on a US Government system for non-government purposes. According to her supervisor, the Deputy Director of the Special Security Directorate, and [redacted] her job at the ODNI requires no database searches within JPAS. The IC IG confirmed with the Defense Manpower Data Center (DMDC) – proponent for JPAS—that [redacted] does not maintain a DNI-based JPAS account. Therefore, every occasion [redacted] used JPAS while at the ODNI was improper. For example, on June 18, 2014, [redacted] used her US Government system to access JPAS and retrieve clearance information on a contractor for Maverick LLC (on a DIA contract). Corresponding emails were then sent from Maverick LLC to Red Arch Solutions, onto DIA, on US Government systems, while on duty at the ODNI. (EXHIBIT V)

b3
b6
b7C - IG Subject
b7E - IG Tech

(U//~~FOUO~~) According to DSS, [redacted] is expected to maintain strict controls on the use of JPAS and any matters related to personally identifiable information (PII) in her role as FSO. The data found on [redacted] US Government system from May 10, 2010 to present is in direct violation of the policies and regulations set forth by DSS. Furthermore, the same policies and regulations that [redacted] violated, are the same policies and regulations that she is expected to train clients on in her role as FSO. Given the familiarity [redacted] has with the security policies and regulations as an FSO, the data found on her US Government system indicates an intentional regard of the rules and regulations she is expected to uphold.

b3
b6
b7C - IG Subject

Regulation Awareness

(U//~~FOUO~~) Each time an employee of ODNI logs onto a work computer, they are required to click "OK" under a banner that reads "This is a US Government system and shall be used for authorized purposes only. All information on this system is the property of the US Government and may not be accessed without prior authorization. Your use of this system may be monitored and you have

[19] [redacted]

b3

no expectation of privacy. Violation of the information system security regulations and guidance may result in discipline by the Agency and the violators may be prosecuted." This banner is provided at the login screen of AIN and CWE.

(U//~~FOUO~~) Similar banners are located in Scattered Castles that read:

> "Access to information in this system is restricted to authorized users for official US Government purposes only. All activity on this system is subject to monitoring. Should the data collected during monitoring provide evidence of criminal activity or activity exceeding privileges, such evidence may be provided to the authorities for use in criminal prosecution, administrative, or other adverse action. By continuing past this point, whether you are an authorized user or not, you expressly consent to this monitoring"
>
> and
>
> "NOTICE: Privacy Act Statement: This system maintains records subject to the Privacy Act, and no disclosures of records in the system shall be made without the prior written consent of the individual to whom the record pertains, except as provided in the Privacy Act declarations of routine use. Reasonable efforts must also be made to notify an individual when any record pertaining to him/her is made available to any person pursuant to court order when such order becomes a matter of public record.
>
> This system shall maintain only such information about an individual as is relevant and necessary to accomplish a legally mandated purpose.
>
> The Privacy Act provides for both civil remedies and for criminal penalties against individual officers for violations of various provisions of the Act.
>
> If you have any questions regarding your obligations under the Privacy Act, please contact your legal advisory office."

(U//~~FOUO~~) [redacted] maintains an alternative work schedule. She works what is referred to as a 5/4/9 schedule in where an employee will work nine days every pay period rather than ten, and work nine and half hour days rather than eight and half hour days, save for one, each pay period. Each day,

b3
b6
b7C - IG Subject

[redacted] accessed Scattered Castles and JPAS (which also has a banner) due to her ODNI and FSO duties. Assuming [redacted] took one day off each pay period—on the conservative end of estimates that means she acknowledged the rules and regulations around 18 USC §1030 at least 3,328 times since her EOD with ODNI.

b3
b6
b7C - IG Subject

(U//~~FOUO~~) Each time a person logs onto JPAS, they must click "Agree" under a banner that reads:

> ATTENTION ALL JPAS USERS
>
> It is a violation of DoD Regulations to share username/password, any Approved Active Public Key Infrastructure (PKI) Certificate, or allow an individual to access another person's JPAS account in any manner or form. Only the authorized account holder is permitted to access/use his/her account. Examples of Approved Active PKI Certificates are Common Access Cards (CAC) and Personal Identity Verification (PIV) cards, to include External Certificate Authority (ECA) cards. There are no combined or "company" JPAS user accounts. Users are required to have their own Approved Active PKI Certificate and JPAS account. Individuals cannot use another person's credentials. If you are not using your own account and certificate that are assigned to you, DISCONTINUE USING JPAS IMMEDIATELY and inform your Industrial Security Representative. Any Account Manager, authorized or unauthorized user who violates JPAS security and account management policies will risk immediate forfeiture and TERMINATION of their JPAS account, regardless of any access requirements that may exist to support mission-critical and job-essential tasks. When you select 'AGREE' at the bottom of this page, you are agreeing to comply with all JPAS administration policies, to include the forfeiture of JPAS access if terms of use are violated.
>
> DATA YOU ARE ABOUT TO ACCESS COULD POTENTIALLY BE PROTECTED BY THE PRIVACY ACT OF 1974. You must:
>
> - Have completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information.
> - Ensure that data is not posted, stored or available in any way for uncontrolled access on any media.
> - Ensure that data is protected at all times as required by the Privacy Act of 1974 (5 USC 552a(I)(3)) as amended and other

applicable DOD regulatory and statutory authority; data will not be shared with offshore contractors; data from the application, or any information derived from the application, shall not be published, disclosed, released, revealed, shown, sold, rented, leased or loaned to anyone outside of the performance of official duties without prior DMDC approval.
- Delete or destroy data from downloaded reports upon completion of the requirement for their use on individual projects.
- Ensure data will not be used for marketing purposes.
- Ensure distribution of data from a DMDC application is restricted to those with a need-to-know. In no case shall data be shared with persons or entities that do not provide documented proof of a need-to-know.
- Be aware that criminal penalties under section 1106(a) of the Social Security Act (42 USC 1306(a)), including possible imprisonment, may apply with respect to any disclosure of information in the application(s) that is inconsistent with the terms of application access. The user further acknowledges that criminal penalties under the Privacy Act (5 USC 552a(I)(3)) may apply if it is determined that the user has knowingly and willfully obtained access to the application(s) under false pretenses.
- The U.S. Department of Defense is committed to making its electronic and information technologies accessible to individuals with disabilities in accordance with Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended in 1999. Send feedback or concerns related to the accessibility of this website to: DoDSection508@osd.mil. For more information about Section 508, please visit the DoD Section 508 website.

UNDER THE PRIVACY ACT OF 1974, YOU MUST SAFEGUARD PERSONNEL INFORMATION RETRIEVED THROUGH THIS SYSTEM.

DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

(U//~~FOUO~~) [redacted] works for approximately [redacted] companies and maintains JPAS accounts with eleven. Each time she entered JPAS, [redacted] was required to acknowledge these banners. [redacted] has entered JPAS sixty-two days since January 1, 2014. During her interview [redacted] explained that she frequently has to re-enter JPAS after automatic logoffs every four minutes. Assuming [redacted] entered (and re-entered) onto JPAS four times[20] each day she logged onto the system, [redacted] acknowledged the above warnings 248 times since the beginning of 2014 alone. Furthermore, as the FSO for the companies she represents, she is expected to train all other employees on the policies and regulations of JPAS, underscoring her fiduciary duty and familiarity with the rules and regulations which she violated.

b3
b6
b7C - IG Subject

Privacy Act Violations

~~(S//NF)~~ [redacted] AIN drive held, among many other files, the following information:

b1
b3
b6
b7C - IG Subject
b7E - IG Tech

[20] Four times in four minute increments is approximately sixteen minutes of JPAS use. Using conservative amounts and circumstances, this assumes that [redacted] used fifteen minutes to perform her work. JPAS records indicate [redacted] actually spent approximately forty minutes to an hour each session she logged into JPAS at ODNI.

b3
b6
b7C - IG Subject

(U//~~FOUO~~)

Company	Number of SF86s
Geographic Services Inc.	45
iKare	3
Link Solutions Inc.	123
Twinsoft Corporation	86
File named "SF86s"	22

(U//~~FOUO~~) The Privacy Act of 1974 requires that "data is not posted, stored or available in any way for uncontrolled access on any media." In the case of the 279 SF86s listed above, [redacted] violated the Privacy Act.

b3
b6
b7C - IG Subject

(U//~~FOUO~~) Between June 10, 2013 and July 2, 2013, [redacted] ran JPAS record searches for Edward Snowden 357 times under three of her accounts (Link Solutions, Augusta Westland, and Twin Soft Corporation) while at ODNI facilities during duty hours. According to the Defense Manpower Data Center's Manual on JPAS Account Management, one of the most common JPAS user violations is "querying the JPAS application for 'celebrity' records." This policy is explicitly forbidden in the manuals for JPAS. In the case of 357 unauthorized JPAS queries, [redacted] violated the Privacy Act. (EXHIBIT X)

b3
b6
b7C - IG Subject

(U//~~FOUO~~) In total, regarding only [redacted] maintenance of records and JPAS queries mentioned above, [redacted] violated the Privacy Act 636 times while at an ODNI facility, acting as an FSO, during duty hours for NCIX.

b3
b6
b7C - IG Subject

Exceeding Access to Systems

(U//~~FOUO~~) Between June 10, 2013, and May 19, 2014, [redacted] ran JPAS record-searches for her own record 442 times under four accounts (Link Solutions, Augusta Westland, 99999 Consulting, and Wheeler Network Design). 324 of the 442 JPAS violations in this case were performed while at ODNI facilities during duty hours. According to the Defense Manpower Data Center's Manual on JPAS Account Management, one of the most common JPAS user violations is "querying the JPAS application for your own record." This policy is explicitly forbidden in the manuals for JPAS. (EXHIBIT X)

b3
b6
b7C - IG Subject

(U//~~FOUO~~) On March 14, 2013, a member of the Office of Security for CIA, spoke with [redacted] after a meeting at NCIX. [redacted] inquired after her

b3
b6
b7C - IG Subject

clearance re-adjudication. She witnessed [redacted] search [redacted] for [redacted] own name. She stated that she "tried to hide [her] disbelief" in order to observe how much access [redacted] had to the database. She stated that she believed [redacted] accesses would have allowed her to know [redacted] When confronted with this information in the interview, [redacted] took a lax attitude toward the violation. She admitted that she queried her own record. [redacted] shrugged, explained that [redacted] did not hold enough information to be considered important to her, and that "everybody" runs queries on their own records. [redacted] strictly states, "Agency personnel authorized to handle OS personnel security information as part of their official duties are expected to review the information only on a definite "need-to-know" basis..." On March 14, 2013, [redacted] violated [redacted].

b3
b6
b7C - IG Subject

(U//~~FOUO~~) On May 20, 2014, the IC IG was alerted by the Deputy Director of the Special Security Directorate that [redacted] was found to have downloaded illegal executables on her computer. When confronted, [redacted] strongly denied the accusation and attempted to blame other members of the IT staff or security personnel. In a risk assessment of [redacted] by NCIX, management stated, "Her actions also reflect a pattern of poor judgment and a willingness to break the rules. For example, when [redacted] AIN user account was found to have several unauthorized executable files (programs) including game programs, she denied any knowledge of how the programs were installed on her computer and denied ever playing the games. She attempted to blame the desktop support personnel saying the programs may have been installed when they were installing software for her DOD CAC card reader."

b3
b6
b7C - IG Subject

(U//~~FOUO~~) On August 6, 2014, JPAS suspended all of [redacted] JPAS accounts until further notice and notified companies with which she is associated due to the issues discussed above. JPAS representatives –through DMDC—have emphasized the seriousness of the violations committed by [redacted] by explaining that one instance of the actions taken by [redacted] discussed above would constitute a JPAS revocation. An administrative investigation by DMDC is underway into [redacted] and the [redacted] companies that she represents.

b3
b6
b7C - IG Subject

Other computer related issues

(U//~~FOUO~~) Several personnel, administrative, and counterintelligence issues were discovered [redacted] aside from criminal violations:

b3
b6
b7C - IG Subject
b7E - IG Tech

(U//~~FOUO~~) [redacted] from October 2010 to March 2013, revealed [redacted] websites that [redacted] used for gaming, for example. (EXHIBIT EE) A counterintelligence analyst remarked of [redacted] in an assessment of the audits from May 2010 to May 2013, "I have highlighted the subject's game playing, and noted the trends. Subject appears to use specific gaming sites for a set period of time and then switches to a new site...There do not appear to be any major gaps in time where subject was not visiting some type of gaming site."

b3
b6
b7C - IG Subject
b7E - IG Tech

(U//~~FOUO~~) [redacted] EXHIBIT BB, CC)

b3
b6
b7C - IG Subject
b7E - IG Tech

(U//~~FOUO~~) [redacted]. (EXHIBIT ZZZ)

(U//~~FOUO~~) When confronted with the issue of illegal executables, games, and inappropriate chats on her account during the interview, [redacted] admitted that she spends approximately "all day" on Facebook and plays games at work from four to six hours per day. She also admitted that she engaged in sexually explicit Sametimes with a contractor for the first year of her employment with ODNI.

b3
b6
b7C - IG Subject

(U//~~FOUO~~) In or around the same time of discovering the illegal executable files on [redacted] system, unrelated to the investigation on [redacted] NCIX – in an effort to lower costs—removed AIN from employees' desks and set up a kiosk in the lobby. For the month of June 2014, [redacted] despite lacking access to AIN in her office, 95% of her computer usage was on the AIN system, including continued communication with her outside employers, highlighting the lack of respect [redacted] has for her duties at ODNI. (EXHIBIT V)

b3
b6
b7C - IG Subject
b7E - IG Tech

CONCLUSION

(U~~//FOUO~~) The allegation that Subject misused government information and information systems is substantiated.

ALLEGATION 5

(U~~//FOUO~~) Subject engaged in sexual misconduct while on duty

(U~~//FOUO~~) Referred to ODNI management – See Exhibit (ZZZ)

RECOMMENDATION

(U~~//FOUO~~) ODNI management should take appropriate action to discipline [redacted] and ensure appropriate security clearance and access reviews occur.

b3
b6
b7C - IG Subject

PREPARED BY:

[redacted]

Investigator

APPROVED BY:

[redacted]

b3
b6
b7C - IG Subject

Assistant Inspector General
for Investigations

LIST OF EXHIBITS (IN ORDER REFERENCED)

1. EXHIBIT M: [redacted]
2. EXHIBIT AA: [redacted]
3. EXHIBIT DD: [redacted]
4. EXHIBIT CCCC: [redacted] documentation regarding outside activities Part 1
5. EXHIBIT DDDD: [redacted] documentation regarding outside activities Part 2
6. EXHIBIT VV: [redacted] Unclass emails_Personnel Issue_Aug 2013_INV-2013-0034
7. EXHIBIT N: [redacted]
8. EXHIBIT QQQ: [redacted] DNI (2)
9. EXHIBIT WWW: T [redacted] -05MAR14 (ATTACH)-1
10. EXHIBIT XXX: [redacted] r [redacted] -25MAR14
11. EXHIBIT YYY: [redacted] Items 3-25-14
12. EXHIBIT WW: List of Companies with EIN and FEIN
13. EXHIBIT XX: [redacted]
14. EXHIBIT Z: [redacted]
15. EXHIBIT K: [redacted] _2013 to 2014
16. EXHIBIT X: JPAS Records
17. EXHIBIT V: [redacted]
18. EXHIBIT EE: [redacted]
19. EXHIBIT BB: Facebook Games 1 May 2010 to March 2013 [redacted]
20. EXHIBIT CC: Facebook Games 2 May 2010 to March 2013 [redacted]
21. EXHIBIT ZZZ: [redacted]

b1
b3
b6
b7C - IG Subject
b7E - IG Tech