OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 25, 2015

MEMORANDUM FOR: The Honorable Jeh C. Johnson
Secretary

The Honorable Joseph Clancy
Director
United States Secret Service

FROM: John Roth
Inspector General

SUBJECT: Investigation into the Improper Access and Distribution of Information Contained Within a Secret Service Data System

Attached is our memorandum summarizing our investigation into the allegations of improper access and distribution of information contained within a Secret Service data system. The memorandum is furnished for whatever action you consider appropriate.

Should you have any questions regarding the report, please feel free to contact me.

Attachment

CONTAINS PRIVACY ACT INFORMATION – DO NOT DISCLOSE

This memorandum summarizes the investigation the Office of Inspector General undertook regarding the allegation that one or more United States Secret Service (Secret Service) agents accessed, through restricted Secret Service databases, the employment application of an individual who later became a member of Congress, which was then published by the media. We undertook this investigation after referrals from you, the Secret Service, and staff from the Committee on Oversight and Government Reform.

This memorandum is part of a series of reviews the Office of Inspector General is conducting regarding the Secret Service.[1] This was a purely factual review of the conduct of Secret Service personnel regarding a specific incident; our Office of Information Technology Audits will review the Master Central Index (MCI) system to determine the effectiveness of the protections in place to prevent and detect unauthorized access and disclosure of information within MCI. Additionally, the Secret Service data systems will be part of our annual review pursuant to the Federal Information Security Management Act. Our Office of Inspections and Evaluations and our Office of Audits are also conducting work regarding certain Secret Service programs and operations, as well as specific security incidents. At the conclusion of that work we will summarize what we have found and the larger lessons we can learn from them.

We have substantially completed our review of the allegation and have determined that a Secret Service database containing sensitive personally identifiable information (PII) pertaining to Congressman Jason Chaffetz, Chairman of the House Committee on Oversight and Government Reform, was accessed on approximately 60 occasions by Secret Service employees. We have concluded that a vast majority of those who had accessed the information did so in violation of the Privacy Act, as well as Secret Service and DHS policy. Additionally, we identified one individual who acknowledged disclosing information protected by the Privacy Act to an outside source. However,

[1] See, *Memorandum to Secretary Johnson, Investigation into the White House Complex on March 4, 2015* (May 6, 2015) https://www.oig.dhs.gov/assets/Mga/OIG_mga-050615.pdf[oig.dhs.gov; *Management Advisory-Alarm System Maintenance at Residences Protected by the U.S. Secret Service (Redacted) OIG 15-61*(April 20, 2015) http://srvhq11c03-webs/assets/Mgmt/2015/OIG_15-61_Apr15.pdf; *Memorandum to Secretary Johnson, Allegation into Misuse of Secret Service Resources*, (October 17, 2014) https://www.oig.dhs.gov/assets/pr/2014/Allegations-of-Misuse-USSS-Resources-101714.pdf.

because the number of individuals with access to this information was so great, we were unable to identify others who may have disclosed protected information to third parties.

We conducted this investigation from April 2, 2015 to August 21, 2015. Our objectives were to determine: (1) whether Secret Service personnel impermissibly accessed information concerning Chairman Chaffetz' application; (2) the identity of those individuals; (3) whether the information was further disseminated in violation of the Privacy Act; and, (4) what actions, if any, Secret Service management took to prevent unauthorized access of such information.

This investigation was undertaken by OIG personnel, with assistance from members of the Secret Service Office of Professional Responsibility (OPR). We conducted more than 50 interviews, reviewed Secret Service records, and also obtained, pursuant to subpoena, records from a private entity. We conducted a search of the Secret Service email system, reviewed the Master Central Index, reviewed DHS privacy policies, Secret Service privacy and personnel policies, and examined telephone records.

The findings in this report, and its conclusions, consistent with the independence requirements of the *Inspector General Act* and our general practice, are the exclusive product of the Office of Inspector General.[2]

The First Unauthorized Access of Sensitive Information

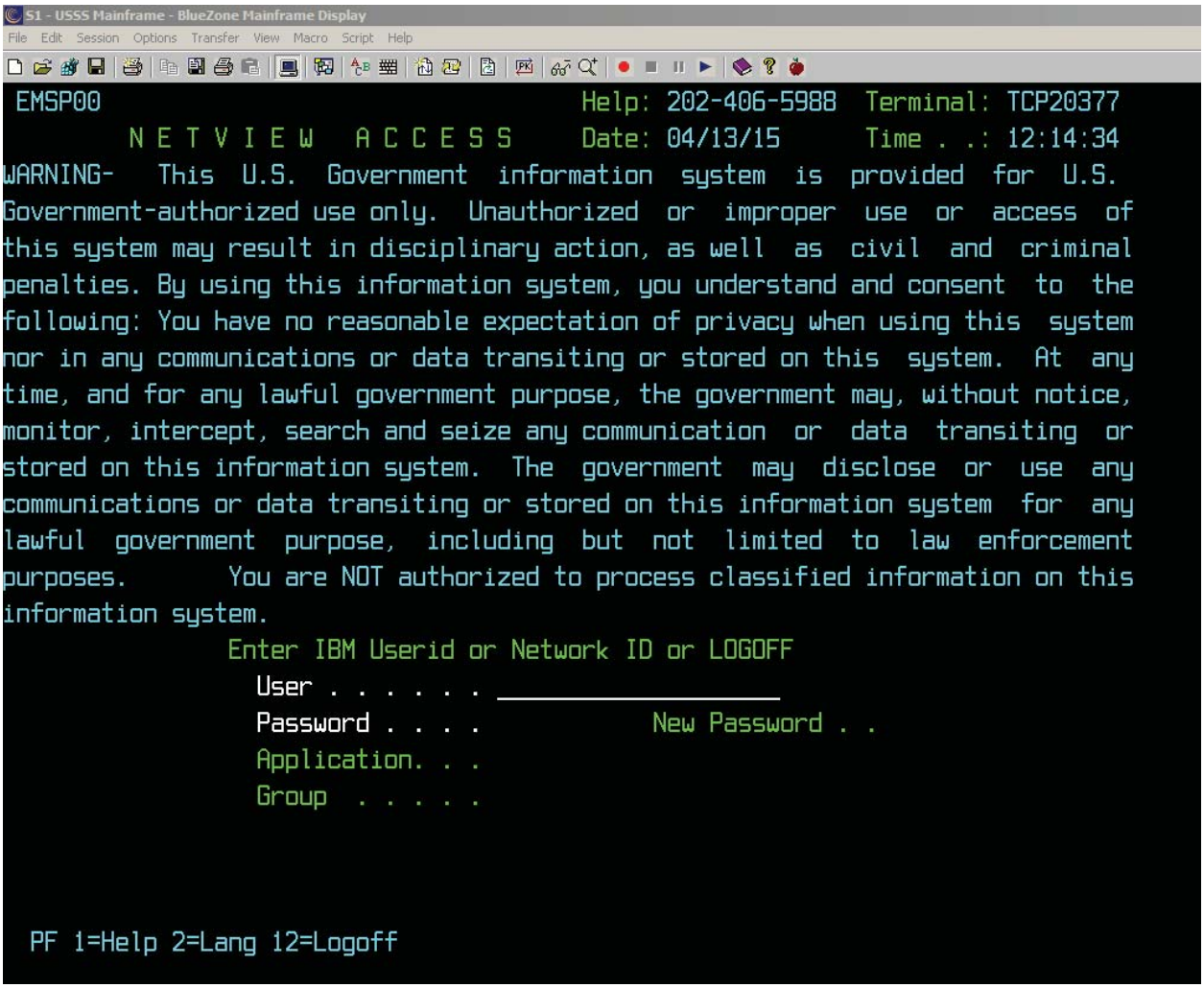
On March 24, 2015, the House of Representatives, Oversight and Government Reform Committee (OGR), conducted a hearing on the actions of the Secret Service on the evening of March 4, 2015, concerning allegations that two Secret Service supervisors breached a crime scene and may have been under the influence of alcohol. The Committee's sole witness was Secret Service Director Joseph Clancy.

The hearing began at approximately10:00 a.m. By 10:18 a.m., a senior Secret Service agent, [redacted], who was an [redacted] assigned to the Office of Administration at Headquarters, holding a grade of GS-14, queried Chairman Jason Chaffetz' name in the MCI Secret Service

[2] The Secret Service, similar to any component that is the subject of a report by this office, was provided an opportunity to review the report prior to publication to identify any information that could compromise its security mission.

database. MCI is a 1980's vintage, electronic database and system of records used by the Secret Service to house agency-unique information, including information on individuals who are the subject of criminal, non-criminal, and protective intelligence investigations, Secret Service personnel and applicant data, and other records such as firearms and physical fitness qualifications.

To access the database, [redacted] would have first logged on with a unique user ID and password, and would have seen the following warning screen:



This warning, which reminds the user that the information contained within the system is for official use only, is necessary because, as we describe below, the information contained within the database is protected by the Privacy Act, applicable to all government data systems that contain information regarding

individuals. Additionally, the database contains sensitive PII, such as dates of birth, Social Security numbers, contact information, and other information that, if improperly disclosed, could lead to personal embarrassment or an increase in the possibility of identity theft or other compromises in personal security. The result of an individual's employment application may also be considered sensitive PII.

The query resulted in Special Agent [redacted] discovering that Chairman Chaffetz, identified by his date of birth, Social Security number, and city of birth, had in fact applied to the Secret Service at the [redacted] Office in September of 2003, but that the application had not been acted upon and the applicant had not been interviewed, reflected in MCI by a data field that read "BQA," which meant that other better qualified applicants existed.

Special Agent [redacted] had no official need to query Chairman Chaffetz' name, because this information was not needed for [redacted] to do [redacted] job. Thus, [redacted] violated the Privacy Act in accessing the information. [redacted] told us [redacted] did so out of curiosity. When [redacted] was interviewed, [redacted] stated that [redacted] was "struck by Chairman Chaffetz' outward animus towards" Director Clancy during his testimony. [redacted] questioned whether there was something else underlying the way Representative Chaffetz treated Clancy, such as Chaffetz having been rejected as an applicant to the Secret Service.

[redacted], upon accessing this information, immediately telephoned Special Agent [redacted], of the Dallas Field Office, where [redacted] used to work. According to [redacted], [redacted] informed him of the fact of the application. [redacted], whose duties largely consisted of investigating applicants, accessed MCI at 10:23 a.m., five minutes after [redacted], and confirmed the fact of the application. [redacted] also shared the information regarding Chairman Chaffetz with [redacted], [redacted], USSS, Presidential Protection Division; [redacted], then-[redacted], Office of Administration; and [redacted], an [redacted] within the Office of Government and Public Affairs. None of these individuals would have had an official purpose in receiving this information. Each subsequent transfer of information, because it came from a Privacy Act-protected record and was made to an individual who had no official need for it, violated the Privacy Act.

[redacted], the Dallas agent who first received the information from [redacted], in turn disclosed the information to Special Agent [redacted], also of the Dallas Field Office, who confirmed the information by searching for Chairman Chaffetz'

name within MCI at 2:23 p.m. that afternoon. [redacted] had no official need to access this record.

By the end of the first day, seven individuals had accessed the record; only one may have had an official purpose in doing so. By the end of the next day, March 25, 2015, an additional 13 personnel had accessed the record; only 2 had an arguable official need for doing so.[3] We were able to determine through an examination of MCI records that in total 45 employees accessed the record approximately 60 times by the time the information was published in the media on April 2, 2015. By our analysis, only four had an arguably legitimate need to do so. A full list of the individuals who accessed Chairman Chaffetz' record in MCI during the time period in question, and the dates and time of their access, is attached as Appendix 1.

Agents accessing the information were located across the country and abroad, including agents working in the following offices:

- Office of Government and Public Affairs;
- Office of Administration;
- Dallas Field Office;
- Office of Training;
- Office of Investigations;
- Phoenix Field Office;
- Presidential Protective Division;
- Charlotte Field Office;
- London Resident Office;
- Office of Strategic Intelligence and Information;
- Washington Field Office (WFO);
- Sacramento Resident Office;
- Office of Human Resources;
- Albany (Georgia) Resident Office;
- Rowley Training Center;

[3] Courts have held that to determine an "official purpose," sufficient to have access to information protected by the Privacy Act, one looks to "whether the official examined the record in connection with the performance of duties assigned to him and whether he had to do so in order to perform those duties properly." Bigelow v. Department of Defense, 217 F.3d, 875, 877 (D.C. Cir. 2000). The best example of an "official purpose" in this instance is the conduct of Deputy Assistant Director Cynthia Wofford, which we describe below.

- Countersurveillance Division;
- San Francisco Field Office;
- Indianapolis Field Office;
- Protective Intelligence Division;
- Special Operations Division;
- William Clinton Protective Division;
- Madison (Wisconsin) Resident Office;
- Houston Field Office;
- Tucson Resident Office;
- Technical Security Division;
- New Haven Resident Office;
- Boston Field Office;
- Investigative Support Division;
- Pittsburg Field Office.

We interviewed each agent who accessed MCI and memorialized the results in a Memorandum of Interview.[4] Pursuant to established policy, the results of those interviews will be given to the Secret Service for whatever personnel action the Secret Service believes is appropriate.

We were unable to determine with certainty how many of those individuals in turn disclosed this information to others who did not have a need to know, who may have then told others. However, the disclosure was widespread, and recipients of the information likely numbered in the hundreds. Those agents we interviewed acknowledged freely sharing it with others in the Secret Service, often contemporaneously with accessing the information. One agent reported that by the end of the second day, he was sent on a protection assignment in New York City for the visit of the President of Afghanistan, and many of the approximately 70 agents at the protection briefing were talking about the issue.

[4] With one exception, every employee interviewed cooperated with the OIG by providing a sworn written statement when requested, as required by DHS Directive 0810.1. One employee, Special Agent [redacted] of the San Francisco Field Office, refused to provide a written statement after his interview. On July 13, 2015, after repeated efforts to obtain a sworn statement, the OIG referred the matter to the Assistant Director, Office of Professional Responsibility. As of the date of issuance of this report, the USSS has not notified the OIG of what action, if any, has been taken for his failure to cooperate as required by the DHS policy.

As we discuss below, Chairman Chaffetz' application was protected by the Privacy Act, and each disclosure of information contained within the MCI to an individual without a need to know it, even if transmitted orally, constituted a violation of the Privacy Act. If the individual knew that it came from a record protected by the Privacy Act, this action exposed the agent and the agency to criminal and civil liability.[5]

Notwithstanding the warning banner and Secret Service policy, many employees insisted that their actions were not inappropriate. A typical response from a GS-13 Special Agent was, "At the time I accessed MCI information I did not think it was inappropriate. If I had known, I would not have accessed the information…. I understand there was a 'banner' when a user logs onto MCI, [but] I did not read it." Some thought that accessing such a record, even to satisfy personal curiosity, was appropriate because it was "our database." However, other employees told us that upon finding the Chaffetz record they immediately realized it was a mistake to have looked for the information, and a number of them self-reported to their supervisor.

E-mail transmission of the MCI screenshot containing sensitive PII

Additionally, agents distributed the information via the Secret Service email system. On the afternoon of the first day, March 24th, Dallas Special Agent [redacted] circulated a screen shot of the MCI record, which contained Chairman Chaffetz' PII, to another Secret Service agent. That agent, Special Agent [redacted] from WFO, distributed the email in turn to two other agents, [redacted] from WFO and [redacted], an Assistant to the Special Agent in Charge from WFO. To the extent we have been able to determine, neither of those agents further distributed the email.

[redacted], a supervisor, was aware that [redacted] had accessed MCI in this fashion, but "didn't think much further about the incident." This email and the chain that followed it – a total of three emails – are the only official Secret Service

[5] We interviewed some agents who recalled that they had heard of the Chaffetz rumors before [redacted] accessed MCI on March 24th. However, none of those agents were able to tell us where they heard the rumor from, or what the source of the rumor was. We were unable to confirm that anyone in the Secret Service had direct knowledge of Chairman Chaffetz' application until it was first accessed by [redacted]. We have concluded that the knowledge of the Chaffetz application originated from the MCI and not any other source.

emails that we found containing the actual MCI record. By embedding the MCI record into an email, which contained sensitive PII such as a social security number and date of birth, [redacted]'s action violated DHS PII policy and increased the risk that Chairman Chaffetz' PII would be compromised. [redacted], [redacted], and [redacted] failed to follow DHS policy when they received the [redacted] email by not immediately reporting the action as a Privacy Incident. In addition, [redacted] and [redacted] violated the Privacy Act as they knew that this information had come from a Privacy Act protected database and that [redacted], [redacted], and [redacted] had no need to know the information.

We also found a number of other emails within the Secret Service system, sent before the publication date of April 2nd, that disclosed the Chaffetz application but did not include his Social Security information or date of birth.

Disclosure Outside of the Secret Service

Two media outlets had apparent access to the fact of Chaffetz' application and the particulars surrounding it, although our investigation did not identify the initial source of their information. The initial publication occurred on the evening of April 2nd by "The Daily Beast," an internet-based news outlet, which reported in an article entitled "Congressman Who Oversees Secret Service Was Rejected by Secret Service" that Chairman Chaffetz had applied to the Secret Service in 2002 or 2003 and had been rejected.[6] It also contained a response from Chairman Chaffetz. Also that evening, the Washington Post published an online article, "DHS asked to probe Secret Service over release of Chaffetz's rejection," which focused on the reaction to the fact that Secret Service agents had improperly accessed Chairman Chaffetz' application.[7] The article reported that senior Congressional staffers had asked DHS to look into the matter and contained responses from Chairman Chaffetz, Ranking Member Cummings, DHS Secretary Johnson, and Director Clancy.

---

[6] See http://www.thedailybeast.com/articles/2015/04/02/congressman-who-oversees-secret-service-was-rejected-by-secret-service.html#, last accessed September 17, 2015.

[7] See http://www.washingtonpost.com/politics/dhs-asked-to-probe-secret-service-over-release-of-chaffetzs-job-rejection/2015/04/02/08352c52-d98e-11e4-b3f2-607bd612aeac_story.html, last accessed September 17, 2015.

Because of the significant number of individuals who had knowledge of Chairman Chaffetz' application history, we were unable to conclusively determine the universe of sources of the disclosure of PII to individuals outside of government. We were also unable to uncover any evidence that particular members of the Secret Service disclosed Chairman Chaffetz' application status to the Daily Beast. With regard to the Washington Post, one agent, [redacted], from WFO, acknowledged in a written statement to OIG that he disclosed, on two separate occasions, information he knew to be derived from Secret Service records, and hence a system of records protected by the Privacy Act, to a Washington Post reporter. He told us that he had confirmed for the reporter the fact that he had received an email that had contained the Chaffetz applicant record.[8] However, [redacted] understood that he was not the sole, or even original, source for this information.

Secret Service Senior Management Awareness of Employee Access

We identified 18 supervisors at the GS-15 or Senior Executive Service level who appeared to have known or should have known, prior to the publication of the fact, that Chairman Chaffetz' MCI record was being accessed. Yet, with a single exception, we found no evidence that any of these senior Secret Service managers attempted to inform the Director or higher levels of the supervisory chain, or to stop or remediate the activity. Furthermore, we found no evidence that a manager at any level issued written guidance for employees to discontinue accessing MCI for anything but official use. Some senior managers, when informed of the fact that agents were accessing MCI for this unofficial purpose, did appropriately counsel the offending employee on the

[8] [redacted] also acknowledged accessing Secret Service data systems that reflected that another agent was on "Do Not Admit" status as a result of an allegation of sexual assault on another employee, and passing that information onto the reporter. This information was protected by the Privacy Act. [redacted] was the only person who accessed that record who did not have an obvious official need for it, and was being investigated separately by the Secret Service Office of Professional Responsibility for that incident and other instances of apparent unauthorized access.

The [redacted] matter was referred to the Department of Justice, which declined prosecution in favor of administrative action. [redacted] has since resigned from the Secret Service.

issue, but it was done orally and without reporting up the chain of command or an attempt to address what was becoming a widespread issue.

One instance is illustrative of what we found. WFO Special Agent in Charge Kathy Michalko became aware on or about March 25th that several of her mid-level WFO supervisors had accessed or were aware of the Chaffetz record. She told us that she did not pass the information to her supervisors at Secret Service Headquarters because she "viewed this matter as specific to WFO and able to be handled at my level," but she directed her subordinates to cease any further access of the MCI record. No other Secret Service personnel at WFO accessed the Chaffetz record after that date, but 25 others around the country did.

Appendix 2 contains a timeline detailing which managers knew about the MCI access and when they knew it.

Similarly, senior managers who knew of the widespread rumors concerning the Chaffetz application should have understood that employees were accessing the MCI applicant record in violation of both Secret Service policy and the Privacy Act and had the potential of causing unfavorable publicity for both the Chairman and the Secret Service. That understanding, in turn, should have caused them to take steps to prevent and mitigate what was occurring.

Additionally, we found two specific instances in which senior managers missed an opportunity either to stop the information themselves, or to inform Secret Service Director Clancy about the Chaffetz record and its improper access by Secret Service employees. These occurred shortly after the initial unauthorized MCI access on March 24th.

Deputy Assistant Director Cynthia Wofford, of the Office of Strategic Intelligence and Information (SII), recalled hearing rumors of the Chaffetz application during the Director's March 24th testimony. After unsuccessfully searching the internet for confirmation of the rumor, Wofford accessed MCI on the morning of March 25th and found the Chaffetz record. Wofford stated in her interview that, in her position overseeing SII, she is charged in part with being aware of any information – such as developing media stories – which may prove embarrassing to the Secret Service, and further, with making notification to the Director or Deputy Director when appropriate.

Wofford told us in her sworn statement that she attempted to brief Deputy Director Craig Magaw about the Chaffetz record in person on or about March 25th. According to her written statement, the Deputy Director "made a shoo-

ing hand motion and stated 'Yeah, yeah we know.' I took this to mean that he didn't want to talk about it any further and that he was well away [sic] of the rumor." Magaw did not discuss this information with the Director at that time. Magaw, for his part, told investigators that he did not recall the exchange.

Also in the middle of the day on March 25th, Dallas Field Office Special Agent [redacted], who was the third person to access the Chaffetz record (and was unauthorized to do so), informed Chief of Staff Michael Biermann during a phone conversation that the Chaffetz applicant record existed in MCI. Biermann, who serves as the de facto gate keeper for the Director and Deputy on many issues, also chose not to pass on this information to either one. He said that by March 25th, he was aware of the rumors regarding Chaffetz earlier that day, although he stated he was not sure where he heard the rumors, other than it came from "the 8th floor" (which is the location of Secret Service senior management). Biermann stated that he was consumed with the issues surrounding the March 4th incident, including the Department and Congressional taskings related to it.

It appears that both Magaw and Biermann were aware of the chatter flowing through their agency, but failed to comprehend the seriousness of what was developing. Neither apparently understood that the rumors were being fueled by, and confirmed by, numerous agents who improperly accessed the protected MCI record of the Chaffetz application. Neither acted, as they certainly had the power to do, to stop this unauthorized and unlawful activity. Each could have issued a directive, deleted or restricted access to the Chaffetz record in MCI, or taken other actions to contain the damage. Neither let the Secret Service Director know.

Moreover, at least one senior Secret Service executive, who knew about the fact of the Chaffetz application, suggested that it be leaked. On March 31st, two days before the publication of the information, Ed Lowery, who is an Assistant Director and in charge of training for the Secret Service, replied to an email from Faron Paramore, another Assistant Director who was in charge of Congressional and public affairs. Paramore's email distributed a press statement by Secretary Johnson regarding Chairman Chaffetz' decision to subpoena Secret Service agents. Lowery's reply, sent only to Paramore, is reprinted in its entirety:

From: EDWARD LOWERY III (TNG)
Sent: Tuesday, March 31, 2015 10:00 PM
To: FARON PARAMORE (ADM)
Subject: Re: STATEMENT BY SECRETARY JEH C. JOHNSON ON THE SUBPOENAS ANNOUNCED BY CHAIRMAN CHAFFETZ

Follow Up Flag: Follow up
Flag Status: Flagged

Some information that he might find embarrassing needs to get out. Just to be fair.
Ed Lowery
Assistant Director
US Secret Service
[redacted]
202-[redacted]
202-[redacted]

From: FARON PARAMORE (ADM)
Sent: Tuesday, March 31, 2015 08:13 PM
To: adstaff
Subject: STATEMENT BY SECRETARY JEH C. JOHNSON ON THE SUBPOENAS ANNOUNCED BY CHAIRMAN CHAFFETZ

Good evening - FYI. Faron.

From: [redacted] [mailto:[redacted]]
Sent: Tuesday, March 31, 2015 08:10 PM Eastern Standard Time
To: FARON PARAMORE (ADM); MICHAEL BIERMANN (DIR)
Subject: Fw: STATEMENT BY SECRETARY JEH C. JOHNSON ON THE SUBPOENAS ANNOUNCED BY CHAIRMAN CHAFFETZ

Lowery, in his interview, denied directing anyone to release information and believed it would have been inappropriate to do so. He described the statement as reflecting his stress and his anger. The recipient of the email, Paramore, stated he never responded to the email and did not act on it. We have no information that would establish that either Lowery or Paramore made good on the email.

Director Clancy told us he did not hear about the Chaffetz application rumor until April 1st and did not know about the improper MCI access until learning of it in connection with the Washington Post article on the evening of April 2nd. Shortly thereafter, on the same evening, the Director had his staff prepare a message addressing the unauthorized release of protected information by Secret Service employees and had the message sent agency-wide that night. This email obliquely referenced the disclosure of the Chaffetz MCI record to the media and reminded employees that they are prohibited from disclosing sensitive agency information, even between Secret Service employees, except pursuant to applicable rules and policies. The message concluded with a

warning that "All dissemination of any such information must immediately cease."

On April 3rd, the Director held a staff meeting with his senior managers to address this issue. On April 17th, the Director issued another all-agency message referring to recent employee misconduct incidents and stated that he will not tolerate employees who continue to disregard rules and violate the oath they once swore to uphold. Those communications are attached as Appendix 3.

Applicable Rules, Regulations and Statutes

Privacy Act

In common terms, the Privacy Act prohibits the government from disclosing records it maintains about an individual to anyone – even inside their own agency – unless that individual consents to disclosure or the disclosure falls within a dozen categories of permissible disclosure. A "disclosure" needn't mean the actual record itself, but can be made by any means, including written, oral or electronic. The exceptions to the prohibition allow an agency to distribute a record without the individual's consent. A disclosure can be made within the agency were an individual has a need for the record in the performance of his or her duties. Other exceptions include responding to a Freedom of Information Act request, for law enforcement purposes under certain conditions, for compelling circumstances involving health and safety, certain Congressional notifications, and other reasons. Other than the "performance of duties" category for Secret Service personnel, none of these exceptions apply to this matter.

Knowing and willful disclosure of material protected by the Privacy Act is a crime. 5 U.S.C. 522a(i)(1). Such a prosecution would require proof that the individual knew that the material was protected by the Privacy Act but nonetheless disclosed it.

Additionally, violation of the Privacy Act exposes the agency to civil liability, in the form of injunctive relief or money damages, if the agency is found to have acted in an intentional or willful manner. 5 U.S.C. § 552a(g)(1)(D). The

legislative history indicates that the standard "is viewed as only somewhat greater than gross negligence."[9]

DHS and Secret Service Policies

Secret Service policies include the Secret Service Information Technology (IT) Rules of General Behavior.[10] Among its provisions, it lists 43 Rules of Behavior and a General Principle that cover employees' use of all Secret Service IT systems. This policy requires Secret Service employees to safeguard sensitive, classified and privacy related information against unauthorized disclosure to the public. It further requires that all Secret Service employees acknowledge review and understanding of the provisions enumerated in that policy upon entering on duty with the Secret Service and annually thereafter. This acknowledgement is memorialized on a standard form and maintained within an employee's personnel record. The Secret Service also has a Table of Penalties to address misconduct including unauthorized use of a government computer and disclosure of information in violation of the Privacy Act. Appendix 4 contains the applicable provisions of these policies.

The March 2012 *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* contains policies that apply to all DHS including all Secret Service employees. Social Security numbers are included in the definition of PII which if disclosed could cause substantial harm to an individual.[11]

- Only access or use Sensitive PII when you have a need to know that information, that is, when your need for the information relates to your official duties.
- Never browse files containing Sensitive PII out of curiosity or for personal reasons.

---

[9] "The degree of culpability required is somewhat greater than gross negligence; damages will be assessed against an agency for committing [an] act without grounds for believing it to be lawful, or … flagrantly disregarding others' rights under the Act." Reuber v. United States, 829 F.2d 133 (D.C. Cir. 1987).
[10] IRM-10(03) (04/23/2007).
[11] (See http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf).

- Share Sensitive PII within DHS if the recipient's need for the information is related to his or her official duties.
- Disclosure of Sensitive PII requires a published routine use under the applicable Privacy Act Systems of Records Notice.
- Employees are required to report to their supervisor all incidents involving unauthorized access or unauthorized disclosure where persons have access to PII for other than an authorized purpose.

The January 2012 DHS Privacy Incident Handling Guidance manual requires DHS personnel to inform their supervisor immediately upon discovery or detection of a Privacy Incident, which includes where an authorized user accesses PII for an unauthorized purpose.[12]

Secret Service policy for contacts with the media is set forth in its Directive System, Government and Public Affairs, GPA-01 issued 11/26/2003. The Public Affairs Program "serves as the spokesman for all official Secret Service policies, issues, policies and procedures…coordinates the receipt and responses to requests for information from the public to the Secret Service…"

As we note in the body of the report, Secret Service personnel violated not only the Privacy Act, but each of these DHS and Secret Service policies.

Conclusion

This episode reflects an obvious lack of care on the part of Secret Service personnel as to the sensitivity of the information entrusted to them. It also reflects a failure by the Secret Service management and leadership to understand the potential risk to the agency as events unfolded and react to and prevent or mitigate the damage caused by their workforce's actions.

All personnel involved – the agents who inappropriately accessed the information, the mid-level supervisors who understood what was occurring, and the senior leadership of the Service – bear responsibility for what occurred. Better and more frequent training is only part of the solution. Ultimately, while the responsibility for this activity can be fairly placed on the shoulders of the agents who casually disregarded important privacy rules, the Secret Service leadership must do a better job of controlling the actions of its personnel. The

[12] (See http://www.dhs.gov/sites/default/files/publications/privacy-incidence-handling-guide.pdf).

Secret Service leadership must demonstrate a commitment to integrity. This includes setting an appropriate tone at the top, but more importantly requires a commitment to establishing and adhering to standards of conduct and ethical and reasonable behavior. Standards of conduct and ethics are meaningful only if they are enforced and if deviations from such standards are dealt with appropriately.

It doesn't take a lawyer explaining the nuances of the Privacy Act to know that the conduct that occurred here – by dozens of agents in every part of the agency – was simply wrong. The agents should have known better. Those who engaged in this behavior should be made to understand how destructive and corrosive to the agency their actions were. These agents work for an agency whose motto – "worthy of trust and confidence" – is engraved in marble in the lobby of their headquarters building. Few could credibly argue that the agents involved in this episode lived up to that motto. Given the sensitivity of the information with which these agents are entrusted, particularly with regard to their protective function, this episode is deeply disturbing.

Additionally, it is especially ironic, and troubling, that the Director of the Secret Service was apparently the only one in the Secret Service who was unaware of the issue until it reached the media. At the March 24th hearing, he testified that he was "infuriated" that he was not made aware of the March 4th drinking incident. He testified that he was "working furiously to try to break down these barriers where people feel that they can't talk up the chain." In the days after this testimony, 18 supervisors, including his Chief of Staff and the Deputy Director, were aware of what was occurring. Yet, the Director himself did not know. When he became aware, he took swift and decisive action, but too late to prevent his agency from again being subject to justified criticism.

APPENDIX 1:

Chronological MCI Access of the Chaffetz Application Record

Title	*Name*	*Assignment*	*Grade*	*Access Date**	*Access Time**
[redacted]	[redacted]	Office of Administration	GS-14	3/24/15	10:18 AM
SA	[redacted]	Dallas Field Office	GS 13	3/24/15	10:23 AM
SA	[redacted]	Dallas Field Office	GS-13	3/24/15	2:23 PM
[redacted]	[redacted]	Office of Administration	GS-14	3/24/15	4:05 PM
SA	[redacted]†	Government and Public Affairs	GS-13	3/24/15	4:53 PM
SA	[redacted]	Office of Investigations	GS-13	3/24/15	5:18 PM
[redacted]	[redacted]	Phoenix Field Office	GS-08	3/24/15	5:20 PM
[redacted]	[redacted]	Presidential Protective Division	GS-11	3/25/15	9:57 AM
[redacted]	[redacted]	Charlotte Field Office	GS-14	3/25/15	10:05 AM
[redacted]	[redacted]	London Resident Office	GS-13	3/25/15	10:07 AM
DAD	Cynthia R. Wofford†	Strategic Intel. and Information	ES-00	3/25/15	10:17 AM
SA	[redacted]	Washington Field Office	GS-13	3/25/15	10:58 AM
SA	[redacted]	Washington Field Office	GS-07	3/25/15	11:21 AM
[redacted]	[redacted]	Washington Field Office	GS-14	3/25/15	11:40 AM
SA	[redacted]	Sacramento Resident Office	GS-13	3/25/15	11:47 AM
SA	[redacted]	Office of Human Resources	GS-13	3/25/15	1:12 PM

Title	*Name*	*Assignment*	*Grade*	*Access Date**	*Access Time**
SA	[redacted]	Charlotte Field Office	GS-13	3/25/15	1:39 PM
[redacted]	[redacted]†	Washington Field Office	GS-14	3/25/15	1:49 PM
[redacted]	[redacted]	Albany (GA) Resident Office	GS-14	3/25/15	4:25 PM
SA	[redacted]	Washington Field Office	GS-13	3/25/15	9:05 PM
SA	[redacted]	Los Angeles Field Office	GS-13	3/26/15	1:27 PM
[redacted]	[redacted]	Lexington (KY) Resident Office	GS-11	3/26/15	2:39 PM
[redacted]	[redacted]	Rowley Training Center	GS-14	3/27/15	9:56 AM
ASAIC	John R. Rotella, Jr.	Counter-surveillance Division	GS-15	3/27/15	12:02 PM
SA	[redacted]	San Francisco Field Office	GS-13	3/27/15	1:35 PM
SAIC	Gary L. Durham	Indianapolis Field Office	GS-15	3/27/15	2:09 PM
[redacted]	[redacted]	Protective Intelligence Division	GS-14	3/27/15	2:27 PM
SA	[redacted]	Special Operations Division	GS-13	3/28/15	5:39 AM
SA	[redacted]	Special Operations Division	GS-13	3/29/15	1:02 PM
SA	[redacted]	William Clinton Protective Division	GS-13	3/30/15	2:39 PM
[redacted]	[redacted]	Madison (WI) Resident Agency	GS-13	3/30/15	5:28 PM
SA	[redacted]	Houston Field Office	GS-13	3/31/15	11:24 AM
SA	[redacted]	Los Angeles Field Office	GS-13	3/31/15	1:24 PM
[redacted]	[redacted]	Houston Field Office	GS-14	3/31/15	5:34 PM

Title	*Name*	*Assignment*	*Grade*	*Access Date**	*Access Time**
SA	[redacted]	Tucson Resident Office	GS-13	3/31/15	7:34 PM
SA	[redacted]	Special Operations Division	GS-13	4/1/15	10:02 AM
SA	[redacted]	Protective Intelligence Division	GS-13	4/1/15	11:44 AM
SA	[redacted]	Vice Presidential Protective Div.	GS-13	4/1/15	12:32 PM
[redacted]	[redacted]	Technical Security Division	GS-13	4/1/15	1:47 PM
SA	[redacted]	New Haven Resident Office	GS-13	4/1/15	2:26 PM
SA	[redacted]	Boston Field Office	GS-13	4/1/15	2:26 PM
[redacted]	[redacted]	Investigative Support Division	GS-14	4/1/15	3:14 PM
SA	[redacted]	Los Angeles Field Office	GS-13	4/1/15	4:44 PM
SAIC	Eric P. Zahren	Pittsburgh Field Office	GS-15	4/2/15	1:06 PM
[redacted]	[redacted]†	Phoenix Field Office	GS-08	4/2/15	6:31 PM

*****This table reflects only the initial query of the Chaffetz record by the above individuals. We were unable to reliably determine the number of times an employee accessed the record within a single session in which an employee was logged into the MCI database. Our investigation determined the above 45 employees accessed the record approximately 60 times.

†These 4 employees were determined to have a legitimate business reason to access the Chaffetz record.

List of Title Abbreviations Used	
AO	Administrative Officer
ASAIC	Assistant Special Agent in Charge
ATSAIC	Assistant to the Special Agent in Charge
DAD	Deputy Assistant Director

List of Title Abbreviations Used	
ISA	Investigative Support Assistant
POS	Protective Operations Specialist
PSS	Protective Support Specialist
RA	Resident Agent
RAIC	Resident Agent in Charge
SA	Special Agent
SAIC	Special Agent in Charge

APPENDIX 2:

Timeline of Senior Management Awareness of Chaffetz Record Access, 3/24/15 – 4/2/15‡

Date/time	Event
3/24 – 10:18 am	First known access of Chaffetz MCI record by [redacted] (GS-14) [redacted], Office of Administration, while watching Director Clancy's testimony on TV.
3/24 – approx. 10 am -12 pm	**DAD Cynthia Wofford** heard rumors of Chaffetz application during Director's testimony, which she was watching on TV.
3/24 - 6:40 pm	SA [redacted], Dallas FO, sent cryptic email to **COS (DAD) Mike Biermann** that he had "some info"; Biermann did not respond until 3/25 (see below).
3/25 – unknown time	SA [redacted], Dallas FO, notified [redacted] (1st line supervisor) of his and [redacted]'s (a former Dallas SA) access. [redacted] questioned why they did this; unknown if he pursued up chain.
3/25 – after 10:05 am	[redacted] of the Charlotte FO accessed record, printed and showed **SAIC Russell Nelson,** Charlotte FO.
3/25 – after 10:07 am	SA [redacted], London RO, accessed record, notified his supervisor, **RAIC (GS-15) Eric Whatley**, London RO.
3/25 – after 10:17 am	**Wofford** briefed **Deputy Director Craig Magaw**, who dismissed her with "Yeah, yeah we know." Wofford stated this occurred "shortly thereafter" she became aware of rumor and looked up record on 3/25. Magaw acknowledged this probably occurred, but did not specifically recall the event.
3/25 – sometime in am	**Biermann** first heard of Chaffetz BQA rumor on "8th Floor" (Senior executive location in USSS Headquarters).
3/25 – around mid-day	**Biermann** returned call to [redacted]; [redacted] told Biermann he wanted to ensure USSS senior management was aware of the Chaffetz applicant record in MCI. [redacted] reported that the record showed Chaffetz had applied to the USSS in 2003 through the [redacted] FO and had been BQA'd for an unknown reason. ([redacted] did not identify the actual date as 3/25, but rather as "several days later" relative to the 3/24 call)

‡ Bolded names are GS-15 or SES level special agents

Date/time	Event
3/25 – 2:24 pm	[redacted], WFO (1st line supervisor), received copy of MCI record embedded in email from SA [redacted], WFO. [redacted] did not make any notifications or otherwise address; claimed to have deleted email.
3/25 – afternoon	**SAIC Kathy Michalko**, WFO, learned of MCI record access when approached by three of her WFO supervisors: [redacted], **ASAIC Martin Mullholland** and **DSAIC James Murray**. Date/time determined relative to access of another WFO supervisor, [redacted]. Michalko addressed issue and ordered subordinates to stop accessing, but did not pass up chain.
3/27 – 11:35 am	**AD Faron Paramore**, GPA, sent **Magaw** email requesting to discuss "recent rumor." Magaw and Paramore both stated this was their first recollection of hearing the Chaffetz application rumor, although Magaw responded to Paramore that he had already heard this before (See Paramore Statement). Paramore stated he was unaware at this time that employees had accessed the MCI record.
3/27 – after 12:02 pm	**ASAIC John Rotella**, Counter-surveillance Division, accessed MCI record, and then self-reported to **SAIC Steven Stanford**. Stanford remarked he shouldn't have done so. Stanford is a direct report to **Wofford**, above, but it does not appear he discussed this with her.
3/27 –2:09 pm	**SAIC Gary Durham**, Indianapolis FO, accessed record personally. Does not appear he passed this up his chain.
3/31 – 10:00 pm	**AD Edward Lowery**, Office of Training, sent email to **AD Paramore** with comment about "embarrassing" information concerning Rep. Chaffetz (i.e. he had knowledge of information contained in the MCI record in order to make this comment). Paramore did not follow-up with Lowery on this comment.
4/1 – 10:30 am	[redacted], Houston FO, accessed MCI record then briefed results at supervisor's meeting on this date. Present were Houston supervisors: **SAIC Cynthia Marble**, **DSAIC Jerald Page, ASAIC Mark McKevitt** and several unidentified ATSAICs.

Date/time	Event
4/1 – after 3:14 pm	[redacted], [redacted], Investigations, accessed record, and "Soon thereafter," notified his supervisors, **ASAIC Sean Scott** and **SAIC Stephen Gasvoda.**
4/1 – unknown time	**Director Joseph Clancy's** first recollection of hearing rumor of Chaffetz application (but not BQA).
4/2 – 1:06 pm	**SAIC Eric Zahren**, Pittsburgh FO, accessed record personally. Zahren did not pass this up his chain.
4/2 – 7:24 pm (or shortly before)	[redacted] notified by email and phone of Washington Post's intent to print article with information from Chaffetz record; [redacted] passed to AD Level at this point.

List of Abbreviations Used	
AD	Assistant Director
ASAIC	Assistant Special Agent in Charge
ATSAIC	Assistant to the Special Agent in Charge
BQA	Better Qualified Applicant (term for applicant rejection)
COS	Chief of Staff
DAD	Deputy Assistant Director
DSAIC	Deputy Special Agent in Charge
FO	Field Office
GPA	Office of Government and Public Affairs
ISD	Investigative Support Division
MCI	Master Central Index (USSS System of Record)
MOA	Memorandum of Activity
RAIC	Resident Agent in Charge
RO	Resident Office
SA	Special Agent
SAIC	Special Agent in Charge
WFO	Washington Field Office

APPENDIX 3:

Director Clancy's Response to Chaffetz Record Access

APRIL 2 EMAIL

From: DIR
Sent: Thursday, April 02, 2015 9:48 PM
To: USA
Subject: 175.040 Handling of Sensitive Information

//Routine//

From: Headquarters (Director) File: 175.040

To: All Employees

Subj: Handling of Sensitive Information

It has recently come to my attention that employees may have accessed and circulated sensitive information concerning an individual. This is to remind and advise all employees that they are prohibited from disclosing any record maintained by this Agency except pursuant to applicable Agency rules and policies. Disclosure of such information between employees is prohibited unless the employee to whom the information is being disclosed has a need for such record in the performance of their duties.

All dissemination of any such information must immediately cease.

Headquarters (Director) Clancy

APRIL 17 EMAIL

From: DIR
Sent: Friday, April 17, 2015 4:11 PM
To: USA
Subject: 175.040 Director's Message

From: Headquarters (Director) File: 175.040

To: All Employees

Subj: Director's Message

Over the past 150 years, the Secret Service has established itself as one the most highly regarded law enforcement agencies in the world. Throughout our history, we have continued to answer the call to serve our country, and through our work, created a tradition of excellence. The cornerstone of our success has always been the selfless dedication to duty displayed by the men and women of this Agency. Having dedicated most of my professional career to the Secret Service, I know that the quality and professionalism of our workforce is without parallel.

Today, the Secret Service is comprised of nearly 6,500 special agents, Uniformed Division officers and administrative, professional and technical personnel. The overwhelming majority of our employees come to work each day, are dedicated to their duties and conduct themselves in a professional manner. However, a small group of individuals continue to disregard the rules and choose to ignore the oath they once swore to uphold. Their behavior tarnishes the reputation of our Agency and I will not tolerate it and I know you will not tolerate it.

I understand that we are all human and that sometimes we make mistakes. However, I do not consider the majority of recent misconduct to be mistakes. Each incident represented a lack of judgement and that is something we can control. As I stated during my testimony on Capitol Hill, everyone - regardless of grade or rank will be held accountable for their actions and behavior. Now is the time for the 99% who represent this Agency honorably, to step forward and pull the 1% up with us. Each of us has a responsibility, not only to the American people, but to each other. Duty, Courage, Honestly, Loyalty and Justice are the values that define this Agency. From this day forward we must reaffirm our commitment to those values, those same values that I am sure your families hold dear.

As a result of alleged and confirmed instances of misconduct, there has been widespread media coverage and intense levels of scrutiny from Congress. We must each recognize that Congress is legislatively mandated to exact oversight on the Secret Service. Just as we do, they also serve the American people. Each member of Congress wants to see this Agency succeed. Whether you agree or disagree with the accuracy of media reporting is irrelevant. The fact is, these incidents occurred and our employees were responsible. Frustration cannot be directed toward any external entity. We must accept responsibility for our errors and commit ourselves to ensuring they do not happen again.

For the last several months, I have met with a large cross-section of our workforce. During my recent visit to the west coast offices, I listened as employees discussed legitimate concerns, challenges and recommendations. I

APRIL 17 EMAIL, CONTINUED:

want each and every employee to know that I am listening to you. In many instances, we have already moved forward to implement new and improved ways of doing business. Some require long-term and systemic changes, but make no mistake; we will continue to change for the better. To that point, it is imperative that I know where problems exist so that the appropriate solutions can be developed. Voicing your concerns through a third party outlet may provide short-term satisfaction but will not correct the problem long-term. My door is open. If there is an issue that needs to be addressed, I encourage you to work with me to identify a solution collaboratively. If you are serious about wanting to enact positive change, then it should start in-house.

This represents a critical time for the Secret Service. Each of us must reevaluate and reaffirm our commitment to our core values and this Agency. If you are personally unable to make that commitment then perhaps this is not the right job for you.

I'm confident that 99% of you are more than willing to make that commitment. I would like to bring that 1% along with us to help us succeed with our mission. However, we are not waiting for everyone to get on board. Our mission is too important. The American people are depending on us. Too many have sacrificed before us, we have too many goals, too much to achieve and too many future experiences to share.

As your Director, I am committed to moving the Secret Service forward and making the necessary changes to ensure the success of our mission and workforce. Our Agency's strength, just as it was 150 years ago, is derived from the quality of our people. Together, we will work to restore our reputation and regain the confidence of the American people.

Thank you for your continued dedication and service.

Headquarters (Director) Clancy

APPENDIX 4:

Applicable Provisions from USSS IT General Rules of Behavior[§] and Table of Penalties[**]

Rule No.	*Text of Rule of Behavior*
General Principle	The following principles apply to all authorized users of Secret Service information resources. Because written guidance cannot cover every contingency, personnel must use their best judgment and highest ethical standards to guide their actions.
3	Users shall protect information from disclosure to unauthorized persons or groups.
26	Users shall not access materials or engage in activities that could post or release sensitive, classified, or privacy related information to the public.
43	Unauthorized or improper use of Government office equipment and information systems/computers may result in the loss of use or limitations on the use of the Internet or Secret Service computers, disciplinary actions, criminal penalties, and/or being held financially liable for the cost of inappropriate use.

Offense Code	*Offense*	*Penalty*
3.6	**Using a government computer or other electronic device for Misuse of Government Computer(s) personal, unofficial, or unauthorized use.** This does not include use of a classified system. This does not apply to de minimis use, i. e., where the cost to the government is negligible, as long as the use is not otherwise objectionable. See 5 C. F. R. § 2635. 704, IRM- 10(03),and ITG- 03(06).	Mitigated: Letter of Reprimand —1 Day Penalty: 3 Days Aggravated: 5 — 14 Days
4.14	**Without authorization, disclosing or attempting to disclose the**	Mitigated: 1— 5 Days

[§] Excerpted from *Information Technology (IT) General Rules of Behavior*, IRM-10(03), United States Secret Service Directives System, 04/23/2007.

[**] Excerpted from *United States Secret Service Table of Penalties*, ITG-04, United States Secret Service Directives System, 12/01/2014.

Offense Code	*Offense*	*Penalty*
	USSS's, or another Agency' s, sensitive material. This also includes Information disclosures of information in violation of the Privacy Act of 1974, 5 U. S. C. § 552a.	Penalty: 7 Days Aggravated: 10 Days — Removal