SECURING PERSONALLY IDENTIFIABLE INFORMATION WITHIN THE UNITED STATES CAPITOL POLICE

HEARING

BEFORE THE

SUBCOMMITTEE ON CAPITOL SECURITY

OF THE

COMMITTEE ON HOUSE ADMINISTRATION

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

HELD IN WASHINGTON, DC, OCTOBER 14, 2009

Printed for the use of the Committee on House Administration

Available on the Internet:
http://www.gpoaccess.gov/congress/house/administration/index.html

U.S. GOVERNMENT PRINTING OFFICE

53–758 WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOUSE ADMINISTRATION

ROBERT A. BRADY, Pennsylvania, *Chairman*

ZOE LOFGREN, California
Vice-Chairwoman
MICHAEL E. CAPUANO, Massachusetts
CHARLES A. GONZALEZ, Texas
SUSAN A. DAVIS, California
ARTUR DAVIS, Alabama

DANIEL E. LUNGREN, California
Ranking Minority Member
KEVIN MCCARTHY, California
GREGG HARPER, Mississippi

JAMIE FLEET, *Staff Director*
VICTOR ARNOLD-BIK, *Minority Staff Director*

SUBCOMMITTEE ON CAPITOL SECURITY

MICHAEL E. CAPUANO, Massachusetts,
Chairman
ROBERT A. BRADY, Pennsylvania

DANIEL E. LUNGREN, California

SECURING PERSONALLY IDENTIFIABLE INFORMATION WITHIN THE UNITED STATES CAPITOL POLICE

WEDNESDAY, OCTOBER 14, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CAPITOL SECURITY,
COMMITTEE ON HOUSE ADMINISTRATION,
Washington, DC.

The subcommittee met, pursuant to call, at 11:02 a.m., in room 1310, Longworth House Office Building, Hon. Michael E. Capuano (chairman of the subcommittee) presiding.

Present: Representatives Capuano and Lungren.

Staff Present: Jamie Fleet, Staff Director; Charles Howell, Chief Counsel; Matt Pinkus, Professional Staff Member, Parliamentarian; Kyle Anderson, Press Director; Greg Abbott, Professional Staff Member; Darrell O'Connor, Professional Staff Member; Shervan Sebastian, Staff Assistant; Matt Field, Minority Professional Staff; and Joe Wallace, Legislative Clerk.

Mr. CAPUANO. First, I want to welcome everybody to the hearing this morning. I want to welcome the Chief and Mr. Hoecker particularly for coming and catching us up on this issue. As I understand, this hearing is being held in relation to H. Res. 40, which relates to the oversight—I forgot about the technology—H. Res. 40, which relates to oversight for various items. And my understanding is today we are going to talk about some PII—I love these initials—personal information, whatever the hell it is, I don't know. And I am basically going to put the official statement on the record because I hate it when these things get read. I am not going to do that. And with that, I am going to ask Mr. Lungren if he wants to do his.

[The statement of Mr. Capuano follows:]

Committee on House Administration
Subcommittee on Capitol Security
Securing Personally Identifiable Information within the U.S. Capitol Police
Wednesday October 14, 2009
Chairman Michael E. Capuano
Opening Statement

Good morning and welcome to the Subcommittee on Capitol Security's hearing on Securing Personally Identifiable Information within the U.S. Capitol Police.

The purpose of this hearing is to perform oversight of the Capitol Police's privacy programs and specifically explore the topic of Personally Identifiable Information – or PII – held by the police. The hearing is also being held in the spirit of H.Res. 40, which passed the House in January of this year and calls for periodic oversight hearings in all House Committees.

Today we will receive an update from the Capitol Police on the status of efforts to address agency privacy concerns and put in place a system for the protection of PII. Identity theft and fraud are significant problems we must guard against in general as more and more personal information is submitted and maintained electronically. The protection of sensitive information should be a priority for all employees with access to such information, particularly in an environment such as Capitol Hill where so many essential government functions take place. I have no doubt that the Capitol Police take that charge very seriously. I look forward today to learning more about their progress in implementing a proper system.

We will hear from Chief Phillip D. Morse of the United States Capitol Police and United States Capitol Police Inspector General Carl W. Hoecker. Chief Morse will detail the agency's privacy protection policies, as well as speak to the work being done to address recommendations from the Inspector General. Mr. Hoecker's testimony will center on the "Audit of USCP Privacy Program" report his office produced in March 2009, in addition to communications he has since had with the Capitol Police about improving policies and procedures.

The Capitol Police continue to do an excellent job protecting Congress and our visitors here on Capitol Hill every day. I know that, while improvements can always be made, the agency keeps the safety of visitors, Members, and staff foremost in mind, and I appreciate the hard work they do.

In closing, I would like to thank House Administration Committee Chairman Brady and Ranking Member Lungren, as well as everyone in the audience for joining us. I look forward to hearing from our witnesses, and I thank them for the time they are taking to be with us today.

Opening Statement [After Capuano's Remarks]

Thank you, Mr. Chairman for calling today's hearing on this important issue.

First, I would like to express my appreciation to the Capitol Police for their effective and efficient protection of the Capitol Complex along with its inhabitants and visitors. This is particularly noted with regard to the recent shooting incident near the Senate Office Buildings. The swift initial defensive actions of the officers involved and the subsequent efforts to prevent further injury to the perpetrator are a credit to both their professionalism and their training.

I am pleased that the Subcommittee is meeting today to address the electronic handling of personally identifiable information. While pieces of information may be stored in separate locations as to decrease the likelihood of association, the interconnectedness of digital systems raises the concern of aggregation by which personnel may be seriously personally

exposed. Despite the challenges, I am confident that a positive working relationship between the Office of the Inspector General and the U.S. Capitol Police can and will be fruitful in implementing proper safeguards.

I look forward to the testimony of our panel of witnesses and thank them for their contribution to our ongoing discussion.

Looking forward, I would request of the Chairman that the future activity of the Subcommittee investigate successes and areas for improvement within the provision of security throughout the Capitol Complex. This extends not merely to the safety of Members and employees, but equally so to the safety of constituents as they visit to learn about, observe, and/or petition the legislative branch of their government.

Thank you, and I reserve the balance of my time.

Mr. LUNGREN. Thank you very much, Mr. Chairman. It is correct that we are calling this meeting pursuant to our requirement for this oversight. I think, first of all, I would like to express my appreciation to the Capitol Police for the great job that they are doing in protecting our visitors and the Members who are here. I think we have passed the 2 million mark now over at the CVC. So we are having a tremendous increase in the number of people who are able to access their Nation's Capitol. But also we had the recent shooting incident near the Senate office buildings. The swift initial defensive actions of the officers involved, as well as the subsequent efforts to prevent further injury to the perpetrator are a credit to both their professionalism and their training. And I think it is good for us to acknowledge that publicly. So Chief, I hope that you will give that message to your people. And I am pleased that we are here dealing with an issue that may sound arcane, but it is rather important. It is what we do with the personal private information of members and staff. When should be it released? Under what circumstances should it be released? How should it be protected? Do we have the means by which we are protecting it? Oftentimes here in this House of Representatives we are busy concerned with the privacy rights of individuals, which is extremely important, but we also ought to take a moment to see how we are handling the privacy information of Members of Congress, which could also relate to their families, and staff here who are helping us. And so I believe that having both the Chief and the inspector general with us will help us to see where we are now and how we might improve, and give some assurance to those with whom we serve as well as those who work with us that we consider their privacy information important as well. So thank you, Mr. Chairman, for having this, and I look forward to the testimony.

Prepared Statement of the Hon. Robert Brady

I would like to thank Chief Morse, and the Inspector General Mr. Carl Hoecker, for being here today.

With identity theft becoming more and more commonplace, the need to protect personally identifying information has become increasingly important. It is obvious that as part of their day-to-day operations, the Capitol Police would have to process personally identifying information. Developing and implementing systems to protect that information is a vitally important component of the mission of the USCP. This is not just vital for Capitol Police employees, but for Members and their staffs as well.

I would like to commend the diligence of the Inspector General in identifying ways to improve information security within the Capitol Police Force. Furthermore, I would like to commend Chief Morse for immediately beginning, and actively implementing, the IG recommendations. I appreciate the seriousness with which your department has treated this matter.

Today, I look forward to hearing how the Capitol Police have already begun to safeguard sensitive information, and what improvements we can expect down the road. I want to ensure Members and their staffers that their personal information is safe in the hands of the U.S. Capitol Police.

STATEMENTS OF PHILLIP D. MORSE, SR., CHIEF, UNITED STATES CAPITOL POLICE; AND CARL W. HOECKER, INSPECTOR GENERAL, UNITED STATES CAPITOL POLICE

Mr. CAPUANO. Chief.

STATEMENT OF PHILLIP MORSE, SR.

Chief MORSE. Good morning, Chairman, and good morning, Mr. Lungren. I appreciate the opportunity to testify before you today on personally identifiable information, or PII, of the department's stakeholders. In addition to insuring the privacy of our employees, the United States Capitol Police has the unique responsibility of insuring the privacy of the Members of Congress, congressional staff, and members of the public with whom we have reason to come in contact. Also the U.S. Capitol Police maintain some Department employee PII. The most sensitive employee information is primarily maintained by cross-servicing partner agencies. We actively and continually work with our partners to protect this employee PII. In addition to carrying out our mission, the department's policy is to secure and maintain very limited personally identifiable information on Members of Congress, such as names, residences, addresses, and contact numbers. The Department also securely maintains PII that is collected for law enforcement purposes involving the public.

The Department has various policies, procedures, and protocols in place to ensure that PII collected in these various areas is necessary, reasonable, appropriately secured, and properly maintained. Earlier this fiscal year, the U.S. Capitol Police Office of Inspector General conducted an audit on the Department's privacy program. In that audit, the inspector general made three recommendations regarding the measures the Department should take to establish a more unified and formal privacy program to enhance the protection of PII.

As indicated in my response to the inspector general's report, I concur and I embrace all of the recommendations. I am also pleased to convey that we have taken steps to address a number of these issues, and are actively engaged in deploying plans on how to best address the remaining issues. Recently, the Department appointed Mr. Norman Farley as our new chief administrative officer and chief privacy officer. Related to his duties as the Department's chief privacy officer, I have asked Mr. Farley to review all existing policies, procedures, and protocols, addressing privacy-related risks, and developing cohesive guidance to assist in the identification, implementation, and maintenance of a unified privacy program in coordination with the Department's executive management team and our Office of General Counsel.

In the short time since his appointment, Mr. Farley has already begun to assess the Department's current activities related to PII, and is slated to provide his findings and implementation plan to the Department's executive team within the next few months. This plan will include establishing timelines and milestones for the full implementation of a unified privacy program within the Department. Although the office of inspector general audit recommendations will remain open until the unified privacy program and policy are finalized and implemented, I am also pleased to report that the corrective actions we have identified to resolve the issues raised in this report have been deemed by the inspector general to be effective approaches to the issue.

I believe that the Department has the initial tools required to effectively and efficiently facilitate the establishment of a unified pri-

vacy program that will mitigate identified privacy-related issues and risks. Please be assured that we are fully committed to executing this plan to ensure the security and privacy of our employees, the public, and Members of Congress and their staffs.

Again I just want to thank you for the opportunity to appear here today, and I am happy to answer any questions that you may have. Thank you.

[The statement of Chief Morse follows:]

Statement of
Phillip D. Morse, Sr.
Chief of Police, United States Capitol Police
Before the
Committee on House Administration
Subcommittee on Capitol Security
United States House of Representatives

October 14, 2009

Chairman Brady and Members of the Committee, thank you for the opportunity to appear before you today to discuss the Department's efforts to protect personally identifiable information of USCP stakeholders.

Personally identifiable information—or PII—is any information that can be used to uniquely and reliably identify an individual. Examples of PII are Social Security numbers, birth dates, home address and telephone numbers, national origin, financial, credit, and medical data. Maintaining the security of PII has become an important issue in an environment where identity theft and fraud are prevalent. Technological advances and the pervasiveness of data collection technologies have further increased the need to be vigilant in the effort to safeguard all PII contained in an agency's various data and records management systems.

In addition to ensuring the privacy of its own employees, the United States Capitol Police has the unique responsibility of ensuring the privacy of Members of

Congress, congressional staff, and members of the public with whom we have reason to come in contact.

Although the U.S. Capitol Police does maintain some Department employee PII, the most sensitive information is primarily maintained by cross-servicing partner agencies. We actively and continuously work with our partners to protect employee PII. In order to carry out our mission, the Department securely maintains very limited personally identifiable information on Members of Congress, such as, names, residence addresses, and contact telephone numbers. The Department also securely maintains PII that is collected for law enforcement purposes involving the public. The Department has various policies, procedures, and protocols in place to ensure that the PII collected in these various areas is necessary, reasonable, appropriately secured, and properly maintained.

Earlier this fiscal year, the U.S. Capitol Police Office of Inspector General conducted an audit of the Department's Privacy Program. In that audit, the OIG made three recommendations regarding measures the Department should take to establish a unified and formal privacy program to enhance the protection of PII. As indicated in my response to the OIG's report, I concur with and embrace all of the recommendations. I am pleased to convey that during the last 90 days we have taken steps to address a number of these issues and are actively engaged in developing plans on how best to address the remaining issues.

Recently, the Department appointed Mr. Norman Farley as the new Chief Information Officer/Chief Privacy Officer. Related to his duties as the Department's Chief Privacy Officer, I have tasked Mr. Farley with reviewing all existing policy, procedures, and protocols, addressing privacy-related risks, and developing cohesive guidance to assist in the identification, implementation, and maintenance of a unified privacy program in coordination with the Executive Management Team and the Office of the General Counsel. In the short time since his appointment, Mr. Farley has already begun to assess the Department's current activities related to PII and is slated to provide his findings and an implementation plan to the Department's Executive Team within the next few months. This plan will include establishing effective dates and milestones for the full implementation of the privacy program.

Additionally, it is our intent to purchase software in Fiscal Year 2010 that will facilitate the identification of servers, databases, records, or documents containing PII. As part of this project, the Department will inventory the sources of all the personally identifiable information it maintains. Milestones for implementation and rollout of the inventory will be included in the Chief Privacy Officer's implementation plan.

The protection of PII is currently a component of the Department's mandatory annual Security Awareness Training. We are eager to create a more comprehensive and targeted training plan in order to heighten awareness regarding the safeguarding of PII as a means to prevent information security breaches. Once the Department's privacy program has been finalized, training materials will be revised to reflect the established

policy and procedures. The Department will implement online privacy training for its employees and contractors and attendance will be tracked in existing internal software and annual refresher privacy training will be a requirement of the program. Milestones for implementation and rollout of the privacy training will be included in the Chief Privacy Officer's implementation plan.

Although the Office of Inspector General audit recommendations will remain open until the privacy program and policy are finalized and implemented, I am pleased to report that the corrective actions we have identified to resolve issues raised in the report have been deemed by the Inspector General to be effective approaches to the issues . I believe that the Department has the initial tools required to effectively and efficiently facilitate the establishment of a privacy program that will mitigate identified privacy-related risks. We are fully committed to executing this plan to ensure the security and privacy of our employees, the public, Members of Congress and their staff.

Thank you again for the opportunity to appear before you today. I am happy to answer any questions you may have.

Mr. CAPUANO. Mr. Hoecker.

STATEMENT OF CARL HOECKER

Mr. HOECKER. Thank you, Mr. Chairman, Mr. Lungren. Good morning. My name is Carl Hoecker. I am the Inspector General for the Capitol Police. Thank you for inviting me here this morning to discuss our work regarding the Department's privacy program. My office conducted an audit of the Department's privacy efforts. The objectives were to determine if the Capitol Police had developed a privacy program that adheres to Federal standards and best practices, and if the program's safeguards assisted the Department in protecting stakeholder information from potential disclosure, specifically that of Congressional Members and their staff. Our scope included the Department's privacy programs in effect as of October 1st, 2008.

We defined the term Personally Identifiable Information, PII, as the information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, et cetera, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, et cetera. While the Capitol Police is a legislative branch agency and generally not required to comply with executive branch regulations, the Department views the principles of the Office of Management and Budget, (OMB), guidance and other sources as best practices to develop its policies and procedures.

Federal privacy best practices require that each Federal agency develop and implement policies and procedures for an overall privacy program; identify and safeguard PII in both paper and electronic form; develop a training program to annually educate employees on requirements for handling PII; perform risk assessments over major information systems and implement appropriate safeguards based upon those risks; and implement secure baseline configurations over information systems. OIG found the Department does not have a formal privacy program that ensures privacy-related risks have been identified and adequately addressed. While the Capitol Police do collect and handle PII of Congressional Members and their staff, the Department has not identified where the PII is collected, maintained, processed, or disseminated. The Department has neither clearly defined the roles and responsibilities of key privacy personnel, nor provided applicable training to such personnel. We also noted that the Capitol Police organizational chart did not identify the Chief Privacy Officer, or CPO, or include this position within its organizational structure. Additionally, the role of the CPO has not yet been defined by the Department. The lack of a CPO position on the organizational chart and the absence of a clear role for the CPO indicate that the position's authority has not been communicated or recognized within the Department.

During the course of our work, OIG noted no instances of either intentional or inadvertent releases of PII. However, the scope of the audit was not designed to identify breaches of PII. The Department appointed a CPO in August of 2007. The Department also had established a privacy board consisting of a CPO and other key personnel. The board's overall objective is to determine the appro-

priate policy, procedures, operational, administrative, and technological issues within the Department that affect individual privacy, as well as data integrity and data interoperability and other privacy matters.

While the board has taken some action to address the privacy concerns, the majority of the actions taken at the time of our audit were either in draft or initial stages, and, therefore, not functioning effectively. To improve the internal efficiency and effectiveness of the Department's PII program, and to assist in safeguarding such information, OIG recommended that the Department finalize its policies and procedures, identify the CPO in the org chart, clearly define roles, responsibilities, and the authorities of the CPO and other key privacy personnel, and to provide applicable privacy training to all contractors and employees. Additionally, we recommended that the Department immediately conduct a review to identify where PII is collected, maintained, processed, and disseminated within the organization. The Department has agreed with the recommendations. Initial steps have been taken by the Department toward improving programs. However, the recommendations are still open. This concludes my testimony. I would be happy to address your questions.

Mr. CAPUANO. Thank you, Mr. Hoecker.

[The statement of Mr. Hoecker follows:]

Mr. Chairman and Members of the Subcommittee:

Good morning, my name is Carl W. Hoecker. I am the Inspector General for the United States Capitol Police (USCP or Department). Thank you for inviting me here today to discuss our work regarding the Department's privacy program.

My office conducted an audit of the Department's privacy efforts. Our objectives were to determine whether (1) USCP had developed a privacy program that adheres to federal standards and best practices and (2) the program's safeguards assisted the Department in protecting stakeholder information from potential disclosure, specifically that of Congressional members and their staff.

Our scope included the Department's privacy program(s) in effect as of October 1, 2008. We defined the term Personally Identifiable Information (PII) as information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information

which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[1]

While USCP, as a legislative branch agency, is generally not required to comply with executive branch regulations, the Department used principles of Office of Management and Budget (OMB) guidance and other sources as best practices to develop its policies and procedures.[2] Federal privacy best practices require each Federal agency to:

1. Develop and implement policies and procedures for an overall privacy program.
2. Identify and safeguard PII in both paper and electronic form.
3. Develop a training program to annually educate employees on the requirements for handling PII.
4. Perform risk assessments over major information systems and implement appropriate safeguards based on those risks.
5. Implement secure baseline configurations over information systems.

OIG found that the Department does not have a privacy program that ensures privacy-related risks have been identified and adequately addressed. While USCP does collect and handle PII of Congressional members and their staff, the Department has not identified where PII is collected, maintained, processed, or disseminated. The Department has neither clearly

[1] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
[2] Title III of the E-Government Act of 2002, Federal Information Security Management Act of 2002, the Federal Privacy Act, and various OMB memoranda.

defined the roles and responsibilities of key privacy personnel nor provided applicable training to such personnel. We also noted USCP's organizational chart did not identify the Chief Privacy Officer (CPO) or include this position within its organizational structure. Additionally, the role of the CPO has not yet been defined by the Department. The lack of a CPO position on the organization chart and the absence of a clear role for the CPO indicate that the position's authority has not been communicated or recognized within the Department.

During the course of our work, OIG noted no instances of either intentional or inadvertent releases of PII. However, the scope of our audit was not designed to identify breaches of PII.

The Department appointed a CPO in August 2007. The Department also had established a Privacy Board (Board) consisting of the CPO and other key personnel. The Board's overall objective is to "Determine appropriate policy, procedures, operational, administrative, and technological issues within the Department that affect individual privacy, as well as data integrity and data interoperability and other Privacy-related matters." While the Board had taken some action to address privacy concerns, the majority of

actions taken at the time of our audit were either in the draft or initial stages and therefore not functioning effectively.

To improve the internal efficiency and effectiveness of the Department's PII program and to assist in safeguarding such information, OIG recommended that the Department finalize its policies and procedures; identify the CPO in its organizational chart; clearly define roles, responsibilities, and authorities of the CPO and other key privacy personnel; and, provide applicable privacy training to all contractors and employees. Additionally, we recommended the Department immediately conduct a review to identify where PII is being collected, maintained, processed, or disseminated within the organization.

The Department has agreed with the recommendations. Initial steps have been taken by the Department toward improving the program; however, the recommendations are still open.

This concludes my testimony. I would be pleased to address your questions.

Mr. CAPUANO. Chief, I am just curious, I am less interested in my own privacy, because I have chosen a public life, and I kind of figure pretty much everything you have anybody can find out is my guess. Is that a reasonable—what do you have on me that I don't already know?

Chief MORSE. The limited information that we have on Members is provided to us in hard copy, not electronically. It is name, address, phone number, those types of things for emergency contact.

Mr. CAPUANO. Okay. That is what I figured. For me, pretty much everything can be found. And I think for most of us that is pretty readily available by junior league person on the Internet. So I am not worried about that. But I am interested in the staff for the very simple reason that they have not chosen the public life. I guess, Mr. Hoecker, I wanted to ask, when audits get done, that is fine. At this point in time are you reasonably satisfied that they are making reasonable progress towards addressing the issues raised?

Mr. HOECKER. Yes, sir, I am. I think they have taken the initial foundations, set the stage. The way that works is when they satisfy or when the Department believes they have satisfied a recommendation, they provide evidence to my office, and we would look at it and make sure that that is kind of where we are coming from. I think they are headed in the right direction, to answer your question, sir.

Mr. CAPUANO. Okay. I think that is what audits always do. I was a little concerned, though, when you said it was a procedures-oriented, if I remember the terms, audit, as opposed to one looking for breaches. At some point, once the proper procedures are in place, who will then check whether to make sure that the procedures actually work or they have to be amended or whatever? Would that be you or the Department itself or both?

Mr. HOECKER. It could be both, sir. What this looked at is since there wasn't a formal policy, what we would do is when there is a policy, we could test it if it is actually being effectively implemented.

Mr. CAPUANO. Because even with the best of policies there is going to be somebody, even the State Department, you know, we read about all the time somebody at the State Department, somebody at the IRS, State level, same thing, somebody will access it inappropriately. And that is bad enough, but then they will oftentimes catch it. I think that is kind of important as well, to have the right procedures, but also have the right investigative tools available after the fact.

Mr. HOECKER. Yes, sir.

Chief MORSE. Yeah, one of the things that the program and policies and procedures will address is internal controls to prevent, obviously, any breaches of personal information, but also to constantly check to ensure that those policies and procedures are followed and updated on a regular basis.

Mr. CAPUANO. What kind of information do you have on the average staff person? Same type of information?

Chief MORSE. Yeah, there is really no reason for us to keep information on any staff, because our emergency notification system is more of a general notification through e-mail and alert systems. Sometimes there may be information that, you know, their names.

But there is really no other reason to have any other information unless there is a police report taken. In the instance of police reports, whenever there is a damage to auto or traffic accident or a crime, generally speaking, those only require a name, and then their addresses and phone numbers and things like that are identified as on file.

And then we have an internal document or police report that identifies them as staff and who they work for and the information that is needed. And then that is maintained in our reports processing section.

Mr. CAPUANO. I heard some mention of the word "biometrics." I mean, you got my DNA on file someplace?

Chief MORSE. I do not.

Mr. CAPUANO. I can't imagine why you would want it, but that is—all right. So at the moment you are not keeping any biometric information on anybody then?

Chief MORSE. Not that I am aware of.

Mr. CAPUANO. I don't know if that is the full answer now, Chief. You are not supposed to be doing it.

Chief MORSE. I do not keep any of that information, no, or collect it.

Mr. CAPUANO. Okay. Thank you. Mr. Lungren.

Mr. LUNGREN. Why do you think they provide the water bottles for you there? Thanks very much for your testimony. Chief, according to your testimony, Mr. Hoecker's testimony, there was appointed by the Department a chief privacy officer in August of 2007, yet Mr. Hoecker's work was done as of October 1, 2008. And I know you have mentioned that you recently appointed a new chief information officer, chief privacy officer. What happened between August 2007 and October 1, 2008, if we didn't have any policies in place at that point in time?

Chief MORSE. Well, I just want to clarify that the Department does have policies and procedures in place. They just don't fall under any unified program or chief information officer, which we plan to do with this new program. So we do have policies and procedures in place at various entities within the police department that collect personal identifiable information on employees.

Mr. LUNGREN. I am just trying to get at, did I misunderstand you, Mr. Hoecker, when you said they didn't have a policy in place?

Mr. HOECKER. I think the clarification is they don't have any PII policy, something that rolls that all up. There may be policies, for instance in the police section, where when you apprehend a suspect and fill out a form, there may be policies that safeguard reports, but there is no overall PII policy.

Mr. LUNGREN. Chief, when you mentioned that you have information, limited information, personally identifiable information on Members of Congress, names, residence addresses, contact telephone numbers and so forth, is that your independently kept record or is that information you get from the CAO or the Speaker's office or someplace?

Chief MORSE. Yeah, the information that I referred to is provided to us in hard copy from the House Sergeant at Arms office and is updated as necessary.

Mr. LUNGREN. So do you maintain a separate file from the Sergeant at Arms?

Chief MORSE. Yes.

Mr. LUNGREN. Does Sergeant at Arms maintain a file do you know?

Chief MORSE. Yes, I would assume they do, because we get a hard copy matrix from them that is updated periodically. It is kept in the command center of headquarters in a safe. And there is a special operating procedure to direct what happens to that information and how it is released or when it is released.

Mr. LUNGREN. Do you have it maintained electronically?

Chief MORSE. We do not. It is only provided to us in hard copy.

Mr. LUNGREN. So you haven't—you don't have any computer list that you can access for Members if you need to get ahold of them in an emergency or something?

Chief MORSE. We do not.

Mr. LUNGREN. Okay. I know that the police department, your office affords a function to Members' district offices. I know you go out there and do reviews, security reviews and so forth, and make recommendations. We have been the beneficiary of that. In the course of that, do you identify individual employees so that you have names and numbers of people at district offices as opposed to just what happens here on the Hill?

Chief MORSE. Yes, we do. And we protect that information.

Mr. LUNGREN. Is that also held in hard copy as opposed to any computer information list?

Chief MORSE. It is held in hard copy.

Mr. LUNGREN. Is there any plan to computerize those things as we do just about everything else?

Chief MORSE. I don't know that we have any plans to do that, but we safeguard it, minimizing the risk that anyone else can access it by having hard copy only. Once you go electronically, then the risks increase that other people can obtain that. So our preference is to maintain it hard copy fashion.

Mr. LUNGREN. Mr. Hoecker, when you did your audit, how did the United States Capitol Police's privacy program compare to other Federal agencies, even though I know those are executive branch agencies?

Mr. HOECKER. Well, sir, I haven't done any audits of other executive branch agencies. But my sense is there is a mixed bag of policies that are in place—specifically dealing with PII versus agencies that don't have that policy. In that regard, I think since the Capitol Police are a police organization, I believe that my judgment would be that there is a significant reduction of that risk because of the nature of a police organization. So that you are dealing with witnesses, you are dealing with subjects on an everyday basis.

Mr. LUNGREN. Chief, with respect to dealing with other law enforcement agencies, do you treat the information that you have on Members any differently than you would with other information you would have dealing with other police organizations?

Chief MORSE. Well, there are seldom times when we, you know, would share information that they don't already have. In other words, we wouldn't provide them any. So as an example, if we are doing a threat case, the bureau has the primary responsibility and

the investigation of that threat case, and we are simply an assisting agency in helping facilitate that investigation. So the information they have they protect, and there is rarely an opportunity or situation that would come up where we needed to provide them with personal information of the person that they are investigating.

Mr. LUNGREN. Now here on the Hill, for I.D. purposes we have I.D. that is created for family members. They have to give certain information for that in order to assure that the person who has the I.D. is the family member. Do you have that information?

Chief MORSE. I can't answer that now. I do not believe that information is provided to us, because I don't believe we are the ones who issue the identification.

Mr. LUNGREN. As far as you know, you do not maintain that information on family members of Members of Congress?

Chief MORSE. I do not believe we do. I can verify that and give it to you for the record.

Mr. LUNGREN. Okay. Mr. Hoecker, any further recommendations for the United States Capitol Police at this time?

Mr. HOECKER. No, sir.

Mr. LUNGREN. Okay. Thank you very much, Mr. Chairman.

Mr. CAPUANO. I just have one last question, Chief. How long do you hang onto these things? When somebody leaves, how long do you hang onto them? Can you give me Tip O'Neill's cell phone number?

Chief MORSE. No.

Mr. LUNGREN. Haven't been able to talk to him recently?

Mr. CAPUANO. Direct line.

Chief MORSE. Once we are given a new hard copy that is updated, the old copy is destroyed. So it is only current members that we would need to contact or respond to their residence in an emergency situation. So that is the only record that we maintain.

Mr. CAPUANO. So when I leave, you are never going to call me again?

Chief MORSE. I will call you, but I guess I will have to get that through somebody else, not my own information.

Mr. CAPUANO. All right. Thank you. I appreciate it. And I appreciate the progress, too. I understand this is what audits do, they show some weaknesses. And the measure is not in the weaknesses, the measure is in the response to identified weaknesses. And I congratulate you for making the IG happy. And by doing so you are making us happy by making progress. So as far as I am concerned, it sounds like you are going in the right direction, and I appreciate the efforts. All set?

Mr. LUNGREN. I am all set. I would just say if you ascend to the Senate, they will probably keep your information while you are over there.

Mr. CAPUANO. Just change it to a different safe. Thank you very much. I really appreciate it. And I appreciate taking time to update us on this and the progress you have made. Thank you very much, gentlemen.

[Whereupon, at 11:28 a.m., the subcommittee was adjourned.]

○