Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System

Washington, D.C.
July 05, 2016

FBI National Press Office
(202) 324-3691

Remarks prepared for delivery at press briefing.

Good morning. I'm here to give you an update on the FBI's investigation of Secretary Clinton's use of a personal e-mail system during her time as Secretary of State.

After a tremendous amount of work over the last year, the FBI is completing its investigation and referring the case to the Department of Justice for a prosecutive decision. What I would like to do today is tell you three things: what we did; what we found; and what we are recommending to the Department of Justice.

This will be an unusual statement in at least a couple ways. First, I am going to include more detail about our process than I ordinarily would, because I think the American people deserve those details in a case of intense public interest. Second, I have not coordinated or reviewed this statement in any way with the Department of Justice or any other part of the government. They do not know what I am about to say.

I want to start by thanking the FBI employees who did remarkable work in this case. Once you have a better sense of how much we have done, you will understand why I am so grateful and proud of their efforts.

So, first, what we have done:

The investigation began as a referral from the Intelligence Community Inspector General in connection with Secretary Clinton's use of a personal e-mail server during her time as Secretary of State. The referral focused on whether classified information was transmitted on that personal system.

Our investigation looked at whether there is evidence classified information was improperly stored or transmitted on that personal system, in violation of a federal statute making it a felony to mishandle classified information either intentionally or in a grossly negligent way, or a second statute making it a misdemeanor to knowingly remove classified information from appropriate systems or storage facilities.

Consistent with our counterintelligence responsibilities, we have also investigated to determine whether there is evidence of computer intrusion in connection with the personal e-mail server by any foreign power, or other hostile actors.

I have so far used the singular term, "e-mail server," in describing the referral that began our investigation. It turns out to have been more complicated than that. Secretary Clinton used several different servers and administrators of those servers during her four years at the State Department, and used numerous mobile devices to view and send e-mail on that personal domain. As new servers and equipment were employed, older servers were taken out of service, stored, and decommissioned in various ways. Piecing all of that back together—to gain as full an understanding as possible of the ways in which personal e-mail was used for government work—has been a painstaking undertaking, requiring thousands of hours of effort.

For example, when one of Secretary Clinton's original personal servers was decommissioned in 2013, the e-mail software was removed. Doing that didn't remove the e-mail content, but it was like removing the frame from a huge finished jigsaw puzzle and dumping the pieces on the floor. The effect was that millions of e-mail fragments end up unsorted in the server's unused—or "slack"—space. We searched through all of it to see what was there, and what parts of the puzzle could be put back together.

FBI investigators have also read all of the approximately 30,000 e-mails provided by Secretary Clinton to the State Department in December 2014. Where an e-mail was assessed as possibly containing classified information, the FBI referred the e-mail to any U.S. government agency that was a likely "owner" of information in the e-mail, so that agency could make a determination as to whether the e-mail contained classified information at the time it was sent or received, or whether there was reason to classify the e-mail now, even if its content was not classified at the time it was sent (that is the process sometimes referred to as "up-classifying").

From the group of 30,000 e-mails returned to the State Department, 110 e-mails in 52 e-mail chains

Recent National Press Releases

07.05.16 **Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System**

06.28.16 **FBI and Department of State Announce a Global Law Enforcement Forum on Diamond Trafficking and Illicit Trade Hosted by Europol**

06.24.16 **Site Selected for FBI Central Records Complex in Frederick County, Virginia**

06.23.16 **Joshua Skule Named Executive Assistant Director for the Intelligence Branch**

06.22.16 **National Health Care Fraud Takedown Results in Charges Against 301 Individuals for Approximately $900 Million in False Billing**

06.13.16 **Laura Bucheit Named Assistant Director for the Security Division**

06.09.16 **Todd McCall Named Assistant Director for the Operational Technology Division**

05.17.16 **Rising Homicide Rates: The View From the FBI**

05.16.16 **Two Men Extradited from Mexico and Charged with Participation in Murder of ICE Special Agent Jaime Zapata and Attempted Murder of ICE Special Agent Victor Avila**

05.16.16 **FBI Releases 2015 Preliminary Statistics for Law Enforcement Officers Killed in the Line of Duty**

More National Press Releases

From the group of 30,000 e-mails returned to the State Department, 110 e-mails in 52 e-mail chains have been determined by the owning agency to contain classified information at the time they were sent or received. Eight of those chains contained information that was Top Secret at the time they were sent; 36 chains contained Secret information at the time; and eight contained Confidential information, which is the lowest level of classification. Separate from those, about 2,000 additional e-mails were "up-classified" to make them Confidential; the information in those had not been classified at the time the e-mails were sent.

The FBI also discovered several thousand work-related e-mails that were not in the group of 30,000 that were returned by Secretary Clinton to State in 2014. We found those additional e-mails in a variety of ways. Some had been deleted over the years and we found traces of them on devices that supported or were connected to the private e-mail domain. Others we found by reviewing the archived government e-mail accounts of people who had been government employees at the same time as Secretary Clinton, including high-ranking officials at other agencies, people with whom a Secretary of State might naturally correspond.

This helped us recover work-related e-mails that were not among the 30,000 produced to State. Still others we recovered from the laborious review of the millions of e-mail fragments dumped into the slack space of the server decommissioned in 2013.

With respect to the thousands of e-mails we found that were not among those produced to State, agencies have concluded that three of those were classified at the time they were sent or received, one at the Secret level and two at the Confidential level. There were no additional Top Secret e-mails found. Finally, none of those we found have since been "up-classified."

I should add here that we found no evidence that any of the additional work-related e-mails were intentionally deleted in an effort to conceal them. Our assessment is that, like many e-mail users, Secretary Clinton periodically deleted e-mails or e-mails were purged from the system when devices were changed. Because she was not using a government account—or even a commercial account like Gmail—there was no archiving at all of her e-mails, so it is not surprising that we discovered e-mails that were not on Secretary Clinton's system in 2014, when she produced the 30,000 e-mails to the State Department.

It could also be that some of the additional work-related e-mails we recovered were among those deleted as "personal" by Secretary Clinton's lawyers when they reviewed and sorted her e-mails for production in 2014.

The lawyers doing the sorting for Secretary Clinton in 2014 did not individually read the content of all of her e-mails, as we did for those available to us; instead, they relied on header information and used search terms to try to find all work-related e-mails among the reportedly more than 60,000 total e-mails remaining on Secretary Clinton's personal system in 2014. It is highly likely their search terms missed some work-related e-mails, and that we later found them, for example, in the mailboxes of other officials or in the slack space of a server.

It is also likely that there are other work-related e-mails that they did not produce to State and that we did not find elsewhere, and that are now gone because they deleted all e-mails they did not return to State, and the lawyers cleaned their devices in such a way as to preclude complete forensic recovery.

We have conducted interviews and done technical examination to attempt to understand how that sorting was done by her attorneys. Although we do not have complete visibility because we are not able to fully reconstruct the electronic record of that sorting, we believe our investigation has been sufficient to give us reasonable confidence there was no intentional misconduct in connection with that sorting effort.

And, of course, in addition to our technical work, we interviewed many people, from those involved in setting up and maintaining the various iterations of Secretary Clinton's personal server, to staff members with whom she corresponded on e-mail, to those involved in the e-mail production to State, and finally, Secretary Clinton herself.

Last, we have done extensive work to understand what indications there might be of compromise by hostile actors in connection with the personal e-mail operation.

That's what we have done. Now let me tell you what we found:

Although we did not find clear evidence that Secretary Clinton or her colleagues intended to violate laws governing the handling of classified information, there is evidence that they were extremely careless in their handling of very sensitive, highly classified information.

For example, seven e-mail chains concern matters that were classified at the Top Secret/Special Access Program level when they were sent and received. These chains involved Secretary Clinton both sending e-mails about those matters and receiving e-mails from others about the same matters. There is evidence to support a conclusion that any reasonable person in Secretary Clinton's position, or in the position of those government employees with whom she was corresponding about these matters, should have known that an unclassified system was no place for that conversation. In addition to this highly sensitive information, we also found information that was properly classified as Secret by the U.S. Intelligence Community at the time it was discussed on e-mail (that is, excluding the later "up-classified" e-mails).

None of these e-mails should have been on any kind of unclassified system, but their presence is especially concerning because all of these e-mails were housed on unclassified personal servers not even supported by full-time security staff, like those found at Departments and Agencies of the U.S. Government—or even with a commercial service like Gmail.

Separately, it is important to say something about the marking of classified information. Only a very small number of the e-mails containing classified information bore markings indicating the presence of classified information. But even if information is not marked "classified" in an e-mail, participants

of classified information. But even if information is not marked "classified" in an e-mail, participants who know or should know that the subject matter is classified are still obligated to protect it.

While not the focus of our investigation, we also developed evidence that the security culture of the State Department in general, and with respect to use of unclassified e-mail systems in particular, was generally lacking in the kind of care for classified information found elsewhere in the government.

With respect to potential computer intrusion by hostile actors, we did not find direct evidence that Secretary Clinton's personal e-mail domain, in its various configurations since 2009, was successfully hacked. But, given the nature of the system and of the actors potentially involved, we assess that we would be unlikely to see such direct evidence. We do assess that hostile actors gained access to the private commercial e-mail accounts of people with whom Secretary Clinton was in regular contact from her personal account. We also assess that Secretary Clinton's use of a personal e-mail domain was both known by a large number of people and readily apparent. She also used her personal e-mail extensively while outside the United States, including sending and receiving work-related e-mails in the territory of sophisticated adversaries. Given that combination of factors, we assess it is possible that hostile actors gained access to Secretary Clinton's personal e-mail account.

So that's what we found. Finally, with respect to our recommendation to the Department of Justice:

In our system, the prosecutors make the decisions about whether charges are appropriate based on evidence the FBI has helped collect. Although we don't normally make public our recommendations to the prosecutors, we frequently make recommendations and engage in productive conversations with prosecutors about what resolution may be appropriate, given the evidence. In this case, given the importance of the matter, I think unusual transparency is in order.

Although there is evidence of potential violations of the statutes regarding the handling of classified information, our judgment is that no reasonable prosecutor would bring such a case. Prosecutors necessarily weigh a number of factors before bringing charges. There are obvious considerations, like the strength of the evidence, especially regarding intent. Responsible decisions also consider the context of a person's actions, and how similar situations have been handled in the past.

In looking back at our investigations into mishandling or removal of classified information, we cannot find a case that would support bringing criminal charges on these facts. All the cases prosecuted involved some combination of: clearly intentional and willful mishandling of classified information; or vast quantities of materials exposed in such a way as to support an inference of intentional misconduct; or indications of disloyalty to the United States; or efforts to obstruct justice. We do not see those things here.

To be clear, this is not to suggest that in similar circumstances, a person who engaged in this activity would face no consequences. To the contrary, those individuals are often subject to security or administrative sanctions. But that is not what we are deciding now.

As a result, although the Department of Justice makes final decisions on matters like this, we are expressing to Justice our view that no charges are appropriate in this case.

I know there will be intense public debate in the wake of this recommendation, as there was throughout this investigation. What I can assure the American people is that this investigation was done competently, honestly, and independently. No outside influence of any kind was brought to bear.

I know there were many opinions expressed by people who were not part of the investigation—including people in government—but none of that mattered to us. Opinions are irrelevant, and they were all uninformed by insight into our investigation, because we did the investigation the right way. Only facts matter, and the FBI found them here in an entirely apolitical and professional way. I couldn't be prouder to be part of this organization.