July 5, 2016
Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System

Our investigation looked at whether there is evidence

1. classified information was improperly stored or transmitted on that personal system,
    a. in violation of a federal statute making it a felony to mishandle classified information
        i. either intentionally or
        ii. in a grossly negligent way, or;
2. a second statute making it a misdemeanor to knowingly remove classified information from appropriate systems or storage facilities.

1. Secretary Clinton used several different servers and administrators of those servers during her four years at the State Department, and;
2. used numerous mobile devices to view and send e-mail on that personal domain.

As new servers and equipment were employed,

1. older servers were taken out of service, stored, and decommissioned in various ways.

For example, when one of Secretary Clinton's original personal servers was decommissioned in 2013,

1. the e-mail software was removed.
    a. **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.

    b. The effect was that millions of e-mail fragments end up unsorted in the server's unused—or "slack"—space.

From the group of 30,000 e-mails returned to the State Department,

1. **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.**
2. **Eight of those chains contained information that was Top Secret at the time they were sent;**
3. **36 chains contained Secret information at the time; and**
4. **eight contained Confidential information,**
    a. which is the lowest level of classification.

Separate from those,

5. **about 2,000 additional e-mails were "up-classified" to make them Confidential;**
    a. the information in those had not been classified at the time the e-mails were sent.

The FBI also discovered

1. **several thousand work-related e-mails**
    a. **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.

1. 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.

2. 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

1. 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

2. 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,

1. **agencies have concluded that three of those were classified at the time they were sent or received,**
    a. **one at the Secret level and**
    b. **two at the Confidential level.**

The lawyers doing the sorting for Secretary Clinton in 2014

1. did not individually read the content of all of her e-mails,

as we did for those available to us;

2. instead, they relied on header information and used search terms to try to find all work-related e-mails among the
3. reportedly more than 60,000 total e-mails remaining on Secretary Clinton's personal system in 2014.

It is also likely that there are other work-related e-mails that

1. they did not produce to State and that we did not find elsewhere,

and that are now gone because

2. they deleted all e-mails they did not return to State, and
3. the lawyers cleaned their devices in such a way as to preclude complete forensic recovery.

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

1. there is **evidence that they were extremely careless in their handling of very sensitive, highly classified information**.

For example,

1. **Seven e-mail chains concern matters that were classified at the Top Secret/Special Access Program level when they were sent and received.**
2. **These chains involved Secretary Clinton both sending e-mails about those matters and receiving e-mails from others about the same matters.**
3. **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,**
    a. **should have known that an unclassified system was no place for that conversation.**

In addition to this highly sensitive information,

4. **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**

1. **None of these e-mails should have been on any kind of unclassified system,**
2. **but their presence is especially concerning because all of these e-mails were housed on unclassified personal servers**
3. **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

1. **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,

2. **participants who know or should know that the subject matter is classified are still obligated to protect it.**

With respect to potential computer intrusion by hostile actors,

1. we did not find direct evidence that Secretary Clinton's personal e-mail domain, *in its various configurations since 2009*, was successfully hacked.

But,

2. **given the nature of the system and of the actors potentially involved, we assess that we would be unlikely to see such direct evidence.**
3. **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.**
4. **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.**
5. **She also used her personal e-mail extensively while outside the United States,**
6. **including sending and receiving work-related e-mails in the territory of sophisticated adversaries.**
7. **Given that combination of factors, we assess it is possible that hostile actors gained access to Secretary Clinton's personal e-mail account.**

there is evidence of

1. **potential violations of the statutes regarding the handling of classified information,**

To be clear,

1. this is not to suggest that in similar circumstances,
2. a person who engaged in this activity would face no consequences.

To the contrary,

3. **those individuals are often subject to security or administrative sanctions.**