# While Clinton used home email, State's networks were at risk

October 19 2015, byKen Dilanian

In this Wednesday, Oct. 14, 2015, file photo, Democratic presidential candidate Hillary Rodham Clinton speaks at a rally in Las Vegas. The State Department was among the worst agencies at protecting its computer networks while Clinton was secretary from 2009 to 2013, a situation that continued to deteriorate as John Kerry took office and Russian hackers breached the department's email system, according to independent audits and interviews. (AP Photo/John Locher, File)

Hillary Rodham Clinton has come under fierce criticism for doing

business over personal email while secretary of state, putting sensitive data at risk of being hacked. But her communications may not have been any more secure had she used a State Department email address, judging by years of independent audits that excoriated the department over poor cyber security on Clinton's watch.

The State Department's unclassified email system was breached by hackers linked to Russia last year who stole an unspecified number of emails. The hackers hit a department that was among the worst agencies in the federal government at protecting its computer networks while Clinton was secretary from 2009 to 2013, a situation that continued to deteriorate as John Kerry took office, according to independent audits and interviews.

The State Department's compliance with federal cybersecurity standards was below average when Clinton took over but grew worse in each year of her tenure, according to an annual report card compiled by the White House based on audits by agency watchdogs. Network security continued to slip after Kerry replaced Clinton in February 2013, and remains substandard, according to the State Department inspector general.

In each year from 2011 to 2014, the State Department's poor cybersecurity was identified by the inspector general as a "significant deficiency" that put the department's information at risk. The latest assessment is due to be published in a few weeks.

Clinton, the front-runner for the Democratic presidential nomination, has apologized for her use of a private email server for official business while she was secretary of state. The FBI is investigating whether her home server was breached.

State Department officials don't dispute the compliance shortcomings identified in years of internal audits, but argue that the audits paint a

distorted picture of their cybersecurity, which they depict as solid and improving. They strongly disagree with the White House ranking that puts them behind most other government agencies. Senior department officials in charge of cybersecurity would speak only on condition of anonymity.

"We have a strong cybersecurity program, successfully defeating almost 100 percent of the 4 billion attempted intrusions we experience each year," spokesman Mark Toner said.

Two successive inspectors general haven't seen it that way. In December 2013, IG Steve Linick issued a "management alert" warning top State Department officials that their repeated failure to correct cybersecurity holes was putting the department's data at risk.

Based on an audit by Linick, State scored a 42 out of 100 on the federal government's latest cybersecurity report card, earning far lower marks than the Office of Personnel Management, which suffered a devastating breach last year. State's scores bested only the Department of Health and Human Services and the Department of Housing and Urban Development. State Department officials complain the grades are subjective.

Clinton approved significant increases in the State Department' information technology budgets while she was secretary, but senior State Department officials say she did not spend much time on the department's cyber vulnerabilities. She was aware of State's technological shortcomings but was focused more on diplomacy, her emails show.

Clinton's campaign staff did not respond to repeated and detailed requests for comment.

In late 2014, cyber intruders linked to Russia were able to break into the State Department's email system, infecting it so thoroughly that it had to be cut off from the Internet in March while experts worked to eliminate the infestation.


In this Aug. 10, 2006, file photo, the sign used as the backdrop for press briefings at the U.S. Department of State is seen before a news conference at the State Department in Washington. The State Department was among the worst agencies in the federal government at protecting its computer networks while Hillary Rodham Clinton was secretary from 2009 to 2013, a situation that continued to deteriorate as John Kerry took office and Russian hackers breached the department's email system, according to independent audits and interviews. (AP Photo/Charles Dharapak, File)

Emails released by the State Department from her private server show Clinton and her top aides viewed the department's information

technology systems as substandard.

"State's technology is so antiquated that NO ONE uses a State-issued laptop and even high officials routinely end up using their home email accounts to be able to get their work done quickly and effectively," top Clinton aide Ann-Marie Slaughter wrote in an email to Clinton on June 3, 2011.

Slaughter suggested that someone write an article to point out the deficiencies, but Clinton aide Cheryl Mills argued that doing so might alert hackers to their use of private email.

Under Clinton and Kerry, the State Department's networks were a ripe target for foreign intelligence services, current and former government officials say, echoing the situation at OPM, which last year saw sensitive personnel data on 21 million people stolen by hackers linked to China.

The Russian hackers who broke into State's email system also infiltrated networks at the Defense Department and the White House, officials say, and no clear line can be drawn between their success and State's dismal security record.

But as with OPM, State's inspector general identified many of the same basic cybersecurity shortcomings year after year, and the department failed to correct them, records show.

Officials in the inspector general's office believe the department's cybersecurity shortcomings played a role in the email breach, said two officials familiar with their thinking.

Senior State Department officials disagree. They say the Russian hack was the result of a "well-crafted intelligence operation" designed to look normal to the employee who clicked on the attachment, and it was

unrelated to other cybersecurity deficiencies.

No technology can completely thwart the most sophisticated of such hacks, but one official familiar with State's cyber deficiencies argues that the department's sloppy security means officials can't be sure other breaches haven't gone undetected.

State Department officials say that only email was taken in the hack, and that no sensitive databases were breached. The National Security Agency conducted a classified assessment and deemed the breach significant and severe, two officials say. A State Department official said the assessment concluded there was no way to be sure what the hackers accessed.

Those officials, and many others interviewed for this story, declined to be quoted because they were not authorized to address the matter publicly.

Although the hacked email system was unclassified, State Department personnel regularly use it to communicate very sensitive information, some of which is routinely withheld on national security grounds when the emails are made public. It would be valuable intelligence for a foreign adversary, officials say.

Sen. Patrick Leahy, the ranking Democrat on the committee that funds the State Department, is concerned about cybersecurity problems "that have existed for several years," a senior Leahy aide said, speaking on condition of anonymity because he wasn't authorized to discuss the matter publicly.

While many of the details have been blacked out of the audits, the inspector general has criticized State for not implementing an effective risk management program. Without one, "the department cannot prioritize, assess, respond to, and monitor information security risk,

which leaves the department vulnerable to attacks and threats," the IG wrote in the latest report, issued last October.

There are also examples of sloppy management. For example, in 2012, the IG reported that of 116,821 unclassified email accounts, 5,717 had not been used, 529 had passwords set not to expire, 19,335 had been set not to require passwords, and 6,269 users had not logged into their accounts between 2005 and 2011. Such a large volume of unattached accounts makes it easier for hackers to co-opt one of them without anyone noticing.

In 2013, an inspection by the IG into State's cybersecurity office—the Bureau of Information Resource Management's Office of Information Assurance—found waste and dysfunction. The office required State Department agencies to fill out paper spreadsheets to track system updates, and was "unable to locate information in a timely manner," the report found.

State Department officials responsible for cybersecurity acknowledged that the department had gotten behind in its compliance with standards in the Federal Information Security Management Act, known as FISMA, which requires, for example, that agency systems be certified as secure. Many of the State Department systems had not been certified for many years. Officials say they have made great strides in the last year.

"FISMA is very important, but it is process-oriented, and compliance is judged on meeting the process," not whether data is actually protected, Toner said.

State Department officials argue that their system for continually monitoring its networks for threats, known as iPost, exceeds FISMA's security standards.

The inspector general and the Government Accountability Office concluded, however, that iPost did not provide a true picture of the risk to State's networks.