

# The Washington Times

## What a mess: Hillary's home server as secure as official ones at State Department

By Kellan Howell

Thursday, April 2, 2015

Lost in the controversy over [Hillary Rodham Clinton](#)'s private email server and the possible security issues has been repeated warnings that the [State Department](#)'s official computers remain woefully unprepared for cyberattacks despite repeated warnings from its internal watchdog and outside experts.

Last month, the [State Department](#) had to shut down its internal unclassified email as it was still doing system repair work from a Russian attack it suffered last year. In November, the agency conducted a similar clean-up exercise after Russian hackers invaded its systems, in what federal law-enforcement and intelligence officials say was the “worst ever” cyberattack against a federal agency.

In October — the month Russian hackers took over State's system with malware — its inspector general reported that the [State Department](#) had ignored hundreds of recommendations to improve its cybersecurity over several years, with investigators identifying security weaknesses in more than 100 different systems.

Ironically, experts say, [Mrs. Clinton](#)'s email server at her suburban New York home in Chappaqua might not have been much less secure than the official ones at State, given the lapses at Foggy Bottom.

“Given the fact that every two years the Chinese or the Russians succeed in getting into the State server it's not clear it [[Mrs. Clinton](#)'s server] made that much difference,” said [James Lewis](#), director and senior fellow at the Center for Strategic and International Studies, and a former [State Department](#) employee.

“Most email is not secure, so it's hard to get excited about unclassified emails. If she's writing about foreign policy that is more specific and intelligence matters that would be a bigger deal,” [Mr. Lewis](#) said.

The [State Department](#) said as a matter of policy, it doesn't discuss specific security measures for its IT infrastructure but that it continually upgrades its system to stay ahead of malicious actors.

"The [Department](#) takes seriously its responsibility to safeguard its information and continuously takes steps to ensure information is protected. We are implementing a strategy to harden and modernize the [Department](#)'s infrastructure to better protect its data, not only today and tomorrow, but well into the future," said Julia Straker, a spokeswoman for the [department](#).

When it comes to transferring classified, sensitive communications, the State server is better than one in your backyard, cyberexperts concede.

"A [State Department](#) server is still more secure than a private server," said Bob Gourley, a former chief technology officer of the Defense Intelligence Agency. "They will eventually be found if they are penetrating a [State Department](#) system."

Last month, [Mrs. Clinton](#) said her use of a private email server didn't include any classified information. She said the server hosting the account was in a private building that was protected by the U.S. Secret Service.

According to Mr. Gourley, the problems plaguing the [State Department](#)'s IT systems boil down to one word, "leadership."

A good IT leader should build a roadmap with a strict timeline for security improvement, Mr. Gourley explained, and could look to reports from the Inspector General for guidance. Right now, there's no one at the [State Department](#) taking responsibility for that.

In its most recent audit on cybersecurity, the [State Department](#)'s IG wrote that while the agency had made some strides in improving its security, it still ignored key concerns that had piled up over the years.

"Although we acknowledge the [department](#)'s actions to improve its information security program, we continue to find security control deficiencies in multiple information security program areas that were previously reported in FY 2010, FY 2011, FY 2012, and FY 2013. Over this period, we consistently identified similar control deficiencies in more than 100 different systems," investigators wrote in the audit.

Cybersecurity is more difficult at the [State Department](#) according to some experts because of its large global network — embassies, consulates and political appointees in almost every country around the world, many with different IT policies. Those vulnerabilities make it an attractive target for hackers.

"They get pressure that a lot of the domestic agencies never see," [Mr. Lewis](#) said, pointing out that different embassies and officials use different systems and devices.

But Mr. Gourdy argued that private companies have networks that are just as expansive, which they're able to secure.

“It’s not an acceptable excuse,” he said. “Compare them to say [General Electric], which operates in every country of the globe except Cuba and North Korea, why are they more secure than the [State Department](#)? Because they care and they have more leadership. Compare them to everyone else in the Fortune 500 — some of them are terrible at security, some are great at security, and it comes down to leadership.”

On Wednesday, President Obama released a new set of executive actions to impose sanctions on hackers attacking private companies, calling a state of emergency over the alarming increase of cyberattacks.

But given the track record of cybersecurity at federal agencies, or rather a lack of security, cyberexperts say the president shouldn’t think big government is the solution to the problem.

“There’s not a ton of reason to believe that in general the government is better at this than the private sector,” said Julian Sanchez, a senior fellow at the libertarian Cato Institute, specializing in technology and privacy issues.

“In general cybersecurity is a hard problem and most of the things that need to be addressed are local issues that involve choices that thousands of private network operators have to make,” he said. “When we talk about cybersecurity we tend to focus on policy changes and things the government can do, in a way that gives them disproportionate weight.”