0-Federal News Network-DISA

DISA exposes personal data of 200,000 people

Jason Miller@jmillerWFED

February 20, 2020 6:01 pm

About 200,000 people are getting free credit monitoring services after the Defense Information Systems Agency suffered a data breach. *[Rebuild]*

DoD spokesman Charles Pritchard confirmed the breach occurred after DISA's letters to affected employees started appearing on social media.

"While there is no evidence to suggest that any of the potentially compromised personally identifiable information (PII) was misused, DISA policy requires the agency to notify individuals whose personal data may have been compromised," Pritchard said in an email. "Individuals possibly affected by this incident will receive letters containing initial notification of the situation *[Reinforce]*. They will subsequently receive additional correspondence with information about actions that can be taken to mitigate possible negative impacts. Those actions will include access to free credit monitoring services for all affected by this breach *[Rebuild]*. DISA has conducted a thorough investigation of this incident and taken appropriate measures to secure the network. *[Reinforce]*"

Pritchard did not specify what sort of system was breached or precisely what types of individuals might have been affected — current or former DoD employees, contractors or others.

The DISA letter to the affected population says the breach happened during the May to July 2019 timeframe when personal information, including Social Security numbers, may have been compromised.

"We take this potential compromise very seriously," wrote Roger Greenwell, DISA's chief risk officer and chief information officer, in the

letter. “As a result, we have put additional security measures in place to prevent future incidents and we are adopting new protocols to increase protection of all PII.” *[Rebuild]*

Reuters was first to report the DISA data breach.

Greenwell wrote that along with credit monitoring services, individuals can place a fraud alert with credit reporting companies *[Rebuild]*. He said more details are coming about how to sign up for credit monitoring services.

The cost of the credit monitoring services could be significant. For example, the Office of Personnel Management continues to pay for these services after its 2015 breach, renewing the contract in February 2019 for another 18 months for more than $400 million.

The DISA data breach is one of the largest in recent memory suffered by a federal agency.

In July 2019, security research firm Comparitech compiled all the major public sector breaches since 2014 and found only the Postal Service and the Office of Personnel Management breaches in 2018 and 2015 were larger than this latest DISA breach.

“The thing about government data breaches is the data is usually accurate and it’s usually up to date,” said Paul Bischoff, an editor at Comparitech and a consumer privacy expert, on the Federal Drive with Tom Temin in August. “Government data breaches can be quite severe in terms of how usable the data is to someone who is trying to steal identities.”

In 2018, DoD also reported a data breach of travel records for about 30,000 of its employees.

While there have been fewer major data breaches among federal agencies over the past few years, the risk continues to be significant. A report by the Senate Homeland Security and Governmental Affairs Committee from June found eight agencies were at risk of a data breach because they didn’t comply with federal cybersecurity standards.

“In the most recent audits, the inspectors general found that seven of the eight agencies reviewed by the subcommittee failed to properly protect personally identifiable information,” the report stated. “Five of the eight agencies did not maintain a comprehensive and accurate list of information technology assets. Without a list of the agency’s IT assets, the agency does not know all of the applications operating on its network. If the agency does not know the application is on its network, it cannot secure the application. Six of the eight agencies failed to install security patches.”