TONY GONZALES
23RD DISTRICT, TEXAS

COMMITTEE ON APPROPRIATIONS

SUBCOMMITTEE ON MILITARY CONSTRUCTION, VETERANS AFFAIRS, AND RELATED AGENCIES

SUBCOMMITTEE ON TRANSPORTATION, HOUSING AND URBAN DEVELOPMENT, AND RELATED AGENCIES

Congress of the United States
House of Representatives
Washington, DC 20515–4323

WASHINGTON OFFICE:
1009 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225–4511
WWW.GONZALES.HOUSE.GOV

DISTRICT OFFICES:
6333 DE ZAVALA RD.
SUITE A216
SAN ANTONIO, TX 78249
(210) 806–9920

712 EAST GIBBS ST.
SUITE 101
DEL RIO, TX 78840
(830) 308–6200

103 W CALLAGHAN ST.
FORT STOCKTON, TX 79735
(432) 299–6200

124 HORIZON BLVD.
SOCORRO, TX 79927
(915) 990–1500

2401 GARNER FIELD RD.
BUILDING Q
UVALDE, TX 78801
(830) 333–7410

September 6, 2022

Mr. Kurt Delbene
Assistant Secretary for Information and Technology and Chief Information Officer
U.S. Department of Veterans Affairs
810 Vermont Ave., NW
Washington, D.C. 20420

Dear Assistant Secretary Delbene,

I am writing to express concern over a recent report regarding a weakness in how the Veterans Information Systems and Technology Architecture (VistA) encrypts internal credentials and potential implications of this weakness.

This vulnerability, which was recently identified by a security researcher in health care information technology at the Defcon Security Conference[1], could compromise VistA and allow an attacker on a hospital's network to impersonate a health care provider within it. Possible implications of such an attack include impersonators modifying patient records, submitting diagnoses, or prescribing medications.

Furthermore, I am aware of the ongoing delays in the rollout of the Cerner Electronic Health Records Management (EHRM) system. This rollout, which involves the phasing out of VistA using a new medical records system, has also experienced issues with pilot deployments that have nearly resulted in almost 150 cases in which patients could have potentially been harmed.[2]

Given these events and the importance of securing such crucial data, I request that the VA provide information about the steps that it plans to take to ensure VistA remains safe and secure while the EHRM rollout is implemented.

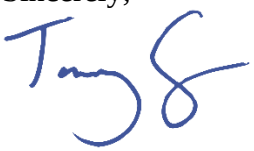
I believe that provider and patient safety is of the utmost priority and should not be compromised under any circumstance. Though the department is working to phase out VistA, the priority to ensure safety should remain at the forefront. In an environment in which cyber-attackers are working to access sensitive and critical information, adequate resources and protection must

[1] A Flaw in the VA's VistA Medical Records Platform May Put Patients at Risk | WIRED
[2] Watchdog reveals flaw in Cerner computer system caused nearly 150 cases of harm at Spokane VA hospital | The Spokesman-Review

be provided to any system that contains this information and ensure that those that served our country are protected.

Thank you and I look forward to your response.

Sincerely,



Tony Gonzales
Member of Congress