

SOV IT Cybersecurity

Chief Information Security Officer John A. Toney

Qualifications & Experience

- Bachelor's degree from Michigan State University
- Executive CISO certification from Carnegie Mellon University, Heinz College of Information Systems and Public Policy
- Nineteen years of government service
- Special Agent with the United States Secret Service
- Originally trained as a hacker by the US Secret Service as part of the Network Intrusion Response (NITRO) program
- Led the Philadelphia Electronic Crimes Task Force (ECTF)
- Cyber investigations instructor at the FBI's International Law Enforcement Academy in Budapest, Hungary
- Served as global Director of incident response, threat intelligence and forensics for Procter & Gamble
- Big 4 consulting alumnus (EY & KPMG)



FBI CISO Academy

FOR INFORMATION SECURITY LEADERS

Dear John,

You are cordially invited to attend the June 2025 iteration of the FBI's Chief Information Security Officer (CISO) Academy. The event brings together CISOs from key industries for a candid dialogue about how the FBI, domestic and international partners, and the private sector can work together to combat the growing threat of cyber attacks. Your perspective and feedback are critical in our mission to secure U.S. national security, infrastructure, and economic interests from cyber attacks.

The upcoming CISO Academy class includes sessions related to cyber investigations, public-private partnership opportunities, and technical tools and techniques used by the FBI to impose costs on our adversaries and defeat cyber threats. Further, speakers will offer attendees insight into how the FBI responds to cyber incidents and conducts cyber intrusion investigations. Attendees will also participate in briefings with government and private sector stakeholders on cybersecurity, incident response, and information sharing. CISO Academy affords participants the opportunity to enhance their analytical and decision-making skills, ensuring participants are delivering a clear message to their Boards of Directors regarding the cyber landscape and partnering with the FBI.

May 7, 2025 | 3

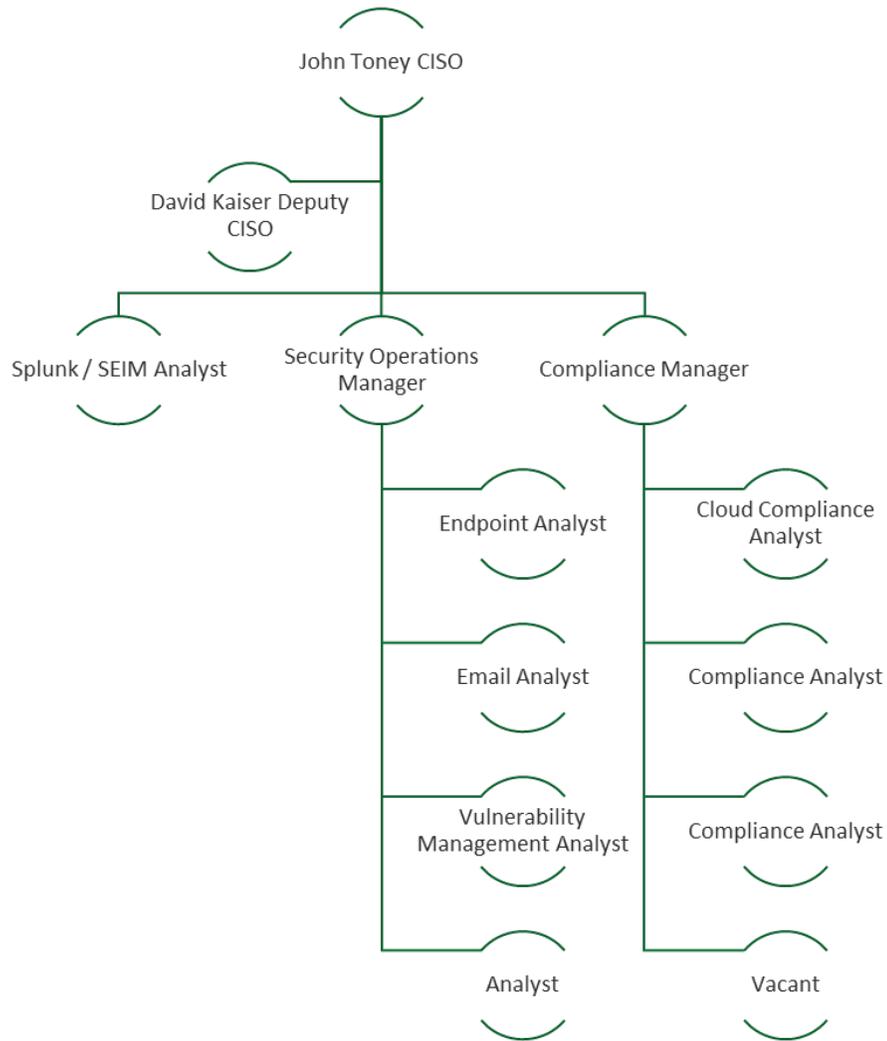


Visiting Fellow

Member of Cyber & Tech Security Council



ADS Information Security Team



Starting with the big number

In 2025, the ADS security team will monitor
358.8 **B**illion events across the State enterprise

Foundations Policy



In November 2024, Vermont's first Information Security Foundations policy was approved and published.

<https://digitalservices.vermont.gov/document/information-security-foundations-policy>

Information Security Foundations Policy

9. DOCUMENT REVISION CONTROL

VERSION NO.	DATE	AUTHOR	COLLABORATORS	DESCRIPTION OF CHANGES
1.0	11/15/2024	ADS Security Office	ADS, AOA, DHR	Released and published to SoV users



Configuration Management



**Information Security
Configuration Management Standard**

6. APPROVAL

NAME/TITLE	DATE	SIGNATURE
John Toney, Chief Information Security Officer – Agency of Digital Services (ADS)	4/28/2025	

7. COMPLIANCE AND CONTROL MAPPING

NIST 800-53	CMS MARS-E	IRS PUB 1075	SSA	HIPAA	CJIS
CM-1	CM-1	CM-1	CM-3	164.308(a)(4)4	CM-1
CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)	CM-2		164.308(a)(8)	CM-2 (1) (2) (3) (7)
CM-3 (2)	CM-3 (2)	CM-3		164.308(a)(7)(i)	CM-3 (2) (4)
CM-4	CM-4 (1) (2)	CM-4		164.308(a)(7)(ii)	CM-4 (2)
CM-5	CM-5 (1) (3) (5)	CM-5		164.308(a)(1)(ii)(D)	CM-5
CM-6	CM-6 (1)	CM-6		164.312(b)	CM-6
CM-7 (1) (2) (4)	CM-7 (1) (2) (5)	CM-7		164.308(a)(5)(ii)(B)	CM-7 (1) (2) (5)
CM-8 (1) (3) (5)	CM-8 (1) (3) (5)	CM-8		164.308(a)(5)(ii)(C)	CM-8 (1) (3)
CM-9	CM-9	CM-9		164.312(e)(2)(i)	CM-9
CM-10	CM-10 (1)	CM-10		164.310(a)(1)	CM-10
CM-11	CM-11	CM-11		164.310(a)(2)(ii)	CM-11

12

On 04/28/2025, I approved our first revision of Configuration Management Standards

DocuSign Envelope ID: 8D89EB7B-6B57-4867-84D1-EFAF018E34E4

				164.310(a)(2)(iii)	CM-12 (1)
				164.310(b)	
				164.310(c)	
				164.310(d)(1)	
				164.310(d)(2)(iii)	
				164.314(b)(2)(i)	
				164.308(a)(3)	
				164.308(a)(4)	

Version: 1.0
Revision Date: 04/28/2025



Cybersecurity events

Email attacks:

In the last 7 days - 6365 attacks were prevented

In the last 30 days - 26,545 attacks were prevented

In the last 9 months - 52,231 attacks were prevented, and 16 made it through our email defense tools

Endpoint defense:

In the last 24 hours, Security noted 210 alerts for triage

In the last 7 days, Security noted 1116 alerts for triage

In the last 30 days, Security noted: 5730 alerts for triage

In the last 90 days, Security noted 41,862 alerts for triage

Security Operations accomplishments

2024 Q1 critical alert response time: 9 minutes

2025 Q1 critical alert response time: N/A (2024 Q4 = > 1 minute)

Time resolution of information security tickets improved 56.3%
over the same period (2024 vs 2025)

Vulnerabilities identified and reduced 75.3% (July 2024 vs. April
2025)

Compliance

- Internal Revenue Service
- Federal Bureau of Investigation
- Health and Human Services
- Social Security Administration
- Federal Emergency Management Administration
- Department of Veterans Affairs
- Centers for Medicare and Medicaid Services
- Cybersecurity & Infrastructure Agency

From the Executive Office of the President (2024)

Hi John,

It was great hearing from you during today's panel at NGA. I thought your inputs were super helpful. Was that other entity?

I want to have discussions with my team here about how we can be more responsive to states' need

Thank you!

Casey Dolen

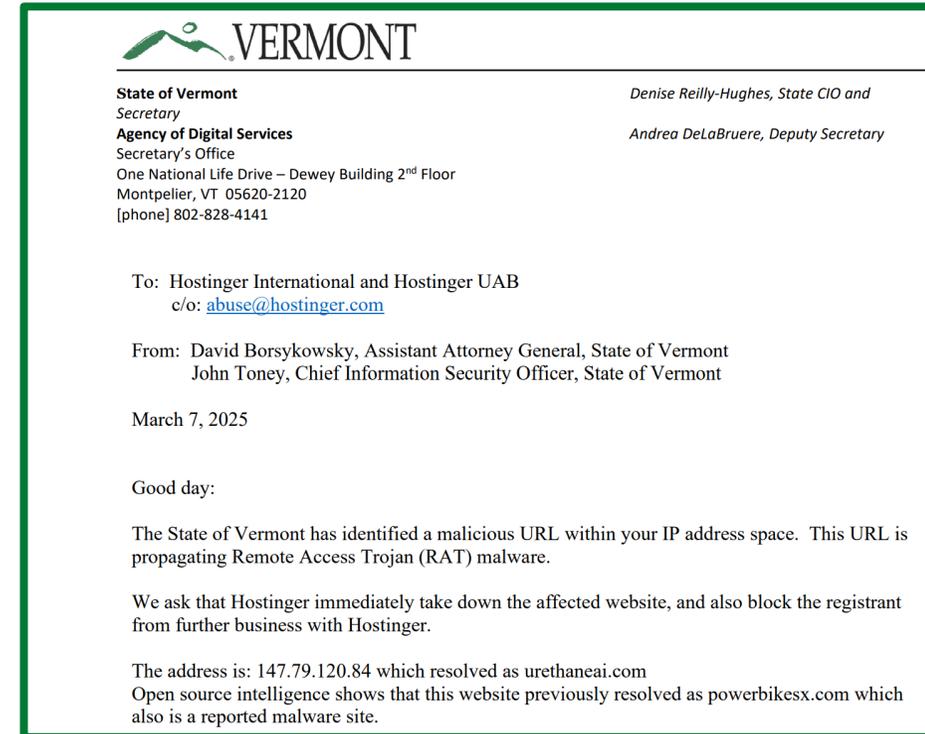
Office of the National Cyber Director

Executive Office of the President

Emerging Threats

Who are the threat actors that we see in Vermont?

- Organized crime
- State sponsored organized crime, to include APT groups (**A**dvanced **P**ersistent **T**hreat)
- Hacktivists
- Unknown actors hiding inside public address space, including Amazon Web Services, Microsoft Azure and small web hosting companies
- Reconnaissance / impersonation of Vermont employees following the use of personal email accounts and other identifiers



What are they actively targeting in Vermont?

- Education and student records (these are most valuable on the dark markets)
- Business email compromise attacks (\$55.5 Billion lost in the last decade globally)
- Traffic cameras & traffic light controllers
- Email accounts
- Credential harvesting
- VT website defacement
- Malware distribution (remote access trojans, ransomware, droppers, banking trojans, account takeover attempts)
- Theft of Personally Identifiable Information and Personal Health Information
- Edge penetration attacks with high volume packet floods

Threat Intelligence

- Threat actors can change Tactics, Techniques & Procedures (TTP's) by the hour, or per use case
- It is reasonable to expect that Vermont will need to be more self sufficient in gathering Threat Intelligence
- Dark web markets (like the former market known as Silk Road) are not static entities. They move and change URL access, so a constant presence is necessary
- Merchants of stolen or hacked data sometimes attempt to sell publicly available data, which must be verified to conduct a proper Incident Response (IR) investigation
- ADS Security is working with the Vermont Intelligence Center and also with the Secretary of State's office to explore a unified threat intelligence platform, so intelligence is shared, and decisions are not made in a vacuum

Collaboration

- Monthly branch coordination calls (Joseph Paquin, John Toney, Marcia Schels, Rain Torres)
- Collaboration with the Vermont State Treasurer's office on controls which directly affect Vermont's bond ratings
- CISO John Toney has assisted the Attorney General's Office in vetting and contracting decisions
- The 2024 general election was secured through close collaboration between ADS Security and the Office of the Secretary of State
- Deputy Chief Information Security Officer, Colonel David Kaiser (United States Air Force, Retired) maintains close collaboration with the National Guard and Vermont State Guard
- Based on his national security experience, CISO John Toney has developed close ties to Vermont Intelligence Center, Vermont State Police and with Vermont Emergency Management