See Something, Say Something in a Digital Age

General (Ret) Paul M. Nakasone
Founding Director
Institute of National Security
Distinguished Research Professor in Engineering Science & Management
Vanderbilt University, Nashville, TN
Paul.m.nakasone@vanderbilt.edu

Brett Goldstein
Special Advisor to the Chancellor
Research Professor in Engineering Science & Management
Vanderbilt University, Nashville, TN
Brett.goldstein@vanderbilt.edu

The United States lacks a coordinated system for individuals to anonymously report cybersecurity threats, creating a critical vulnerability in national security. By applying best practices in secure communications, a unified reporting solution leveraging TOR combined with SecureDrop is both feasible and urgently needed. This position paper evaluates the current cybersecurity reporting landscape, highlights existing gaps, and proposes actionable solutions that can be implemented immediately. Structured to address pressing security challenges, the paper bridges the gap between scholarly research and the longer-term development of policy and legislative frameworks, offering decision-makers a clear path forward.

Keywords: cybersecurity, anonymous reporting, intelligence, detection

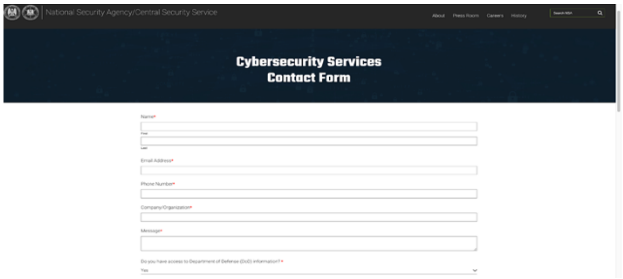
PROBLEM STATEMENT

The U.S. Government currently faces a critical gap in its ability to receive anonymous reports of cybersecurity threats while early detection of cyber-attacks is critical for response (White, 2012). This deficiency hinders intelligence gathering, delays response efforts, and discourages individuals from sharing vital information due to fears of exposure or reprisal. Establishing a secure, anonymous reporting mechanism would enhance the government's situational awareness and bolster national cybersecurity by fostering trust and encouraging broader participation in intelligence-sharing efforts.

The costs of hostile cyber activities vary. According to a 2018 report from The Council of Economic Advisers, malicious cyber activity cost the U.S. economy between $57B and $109B in 2016 (Advisers, 2018). However, the typical cost of a data breach in 2015 was thought to be less than $200,000 (Romanosky, 2016). IBM reports that the global average cost of a data breach in 2024 is 4.88M (IBM, 2024).

CURRENT REPORTING LANDSCAPE

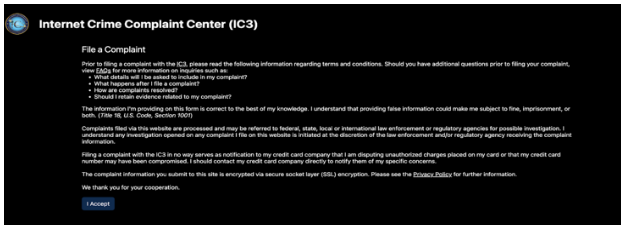
While many federal agencies facilitate and encourage cyber incident reporting (Schwartz, 2022), none offer a secure, anonymous option. Key examples are summarized below for organizations within the intelligence community.



Cybersecurity Services
Contact Form

Name*
First
Last
Email Address*
Phone Number*
Company/Organization*
Message*
Do you have access to Department of Defense (DoD) information? *
Yes

- **National Security Agency Cybersecurity Collaboration Center**: As shown to the left, this is an email-based reporting form that requires personal details that limit the anonymity and security for the submitter. https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Customer-Contact-Form/



Internet Crime Complaint Center (IC3)

File a Complaint

Prior to filing a complaint with the IC3, please read the following information regarding terms and conditions. Should you have additional questions prior to filing your complaint, view FAQs for more information on inquiries such as:

- What details will I be asked to include in my complaint?
- What happens after I file a complaint?
- How are complaints resolved?
- Should I retain evidence related to my complaint?

The information I'm providing on this form is correct to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. (*Title 18, U.S. Code, Section 1001*)

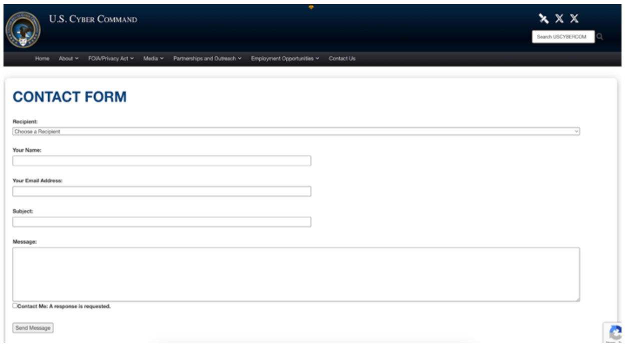
Complaints filed via this website are processed and may be referred to federal, state, local or international law enforcement or regulatory agencies for possible investigation. I understand any investigation opened on any complaint I file on this website is initiated at the discretion of the law enforcement and/or regulatory agency receiving the complaint information.

Filing a complaint with the IC3 in no way serves as notification to my credit card company that I am disputing unauthorized charges placed on my card or that my credit card number may have been compromised. I should contact my credit card company directly to notify them of my specific concerns.

The complaint information you submit to this site is encrypted via secure socket layer (SSL) encryption. Please see the Privacy Policy for further information.

We thank you for your cooperation.

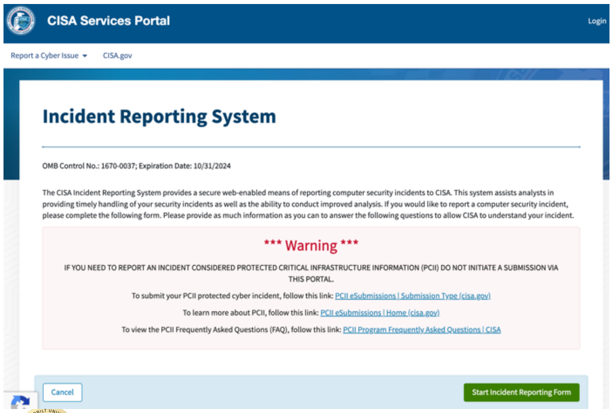
- **Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3):** The Bureau collects cybercrime reports as reflected in their IC3 reporting form on the left but lacks anonymous submission options. https://complaint.ic3.gov/



CONTACT FORM

Recipient:
Choose a Recipient
Your Name:
Your Email Address:
Subject:
Message:
□ Contact Me: A response is requested.

- **U.S. Cyber Command:** While responsible for contributing to overall national cyber defense, Cyber Command does not offer a public reporting mechanism.



Incident Reporting System

OMB Control No.: 1670-0037; Expiration Date: 10/31/2024

The CISA Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the following form. Please provide as much information as you can to answer the following questions to allow CISA to understand your incident.

*** Warning ***

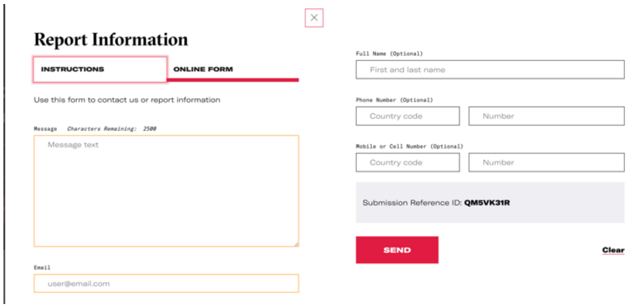
IF YOU NEED TO REPORT AN INCIDENT CONSIDERED PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) DO NOT INITIATE A SUBMISSION VIA THIS PORTAL.

To submit your PCII protected cyber incident, follow this link: PCII eSubmissions | Submission Type (cisa.gov)

To learn more about PCII, follow this link: PCII eSubmissions | Home (cisa.gov)

To view the PCII Frequently Asked Questions (FAQ), follow this link: PCII Program Frequently Asked Questions | CISA

- **Cybersecurity and Infrastructure Security Agency (CISA):** CISA's reporting system focuses on critical infrastructure protection and lacks a secure, anonymous report https://myservices.cisa.gov/irf?id=irf_incident_reporting_start



Report Information

Use this form to contact us or report information

Message *Characters Remaining: 2500*

Message text

Email

user@email.com

Full Name (Optional)

First and last name

Phone Number (Optional)

Country code | Number

Mobile or Cell Number (Optional)

Country code | Number

Submission Reference ID: **QM5VK31R**

- **Central Intelligence Agency (CIA):** The CIA's TOR-based reporting mechanism once heralded for providing robust anonymity (Newman, 2019) is primarily designed for gathering foreign intelligence, not U.S. domestic cybersecurity threats. https://www.cia.gov/report-information

As these examples illustrate, the current reporting landscape shows that reporting options are fragmented and lacks an anonymous, secure system which was further explored in a Department of Homeland 2023 report (Security, Harmonization of Cyber Incident Reporting to the Federal Government, 2023). This gap creates a substantial barrier for individuals reporting cyber incidents.

LIMITATIONS OF CURRENT MECHANISMS

The examples presented above illustrate that there are three primary limitations in the current cybersecurity reporting solutions:

1. **Lack of Uniformity**: Agencies operate isolated reporting systems without centralized coordination. (Office, 2023)

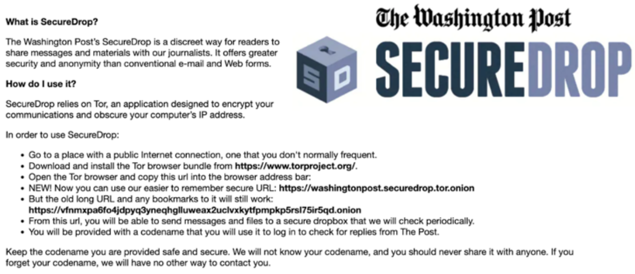
2. **Absence of Anonymity**: Most reporting processes expose submitters' identities, discouraging engagement.

3. **Narrow Scope**: Systems like the CIA's TOR-based platform are not optimized for cybersecurity-specific reporting.

LESSONS FROM SUCCESSFUL MODELS

There are two successful communications and reporting platforms that establish best practices for cyber communications in general.

- **Signal**
  Employs strong end-to-end encryption but retains device linkages, limiting anonymity.



What is SecureDrop?

The Washington Post's SecureDrop is a discreet way for readers to share messages and materials with our journalists. It offers greater security and anonymity than conventional e-mail and Web forms.

How do I use it?

SecureDrop relies on Tor, an application designed to encrypt your communications and obscure your computer's IP address.

In order to use SecureDrop:

- Go to a place with a public Internet connection, one that you don't normally frequent.
- Download and install the Tor browser bundle from **https://www.torproject.org/**.
- Open the Tor browser and copy this url into the browser address bar:
- NEW! Now you can use our easier to remember secure URL: **https://washingtonpost.securedrop.tor.onion**
- But the old long URL and any bookmarks to it will still work: **https://vfnmxpa6fo4jdpyq3yneqhglluweax2uclvxkytfpmpkp5rsl75ir5qd.onion**
- From this url, you will be able to send messages and files to a secure dropbox that we will check periodically.
- You will be provided with a codename that you will use it to log in to check for replies from The Post.

Keep the codename you are provided safe and secure. We will not know your codename, and you should never share it with anyone. If you forget your codename, we will have no other way to contact you.

- **SecureDrop**
Widely used by journalists and other organizations (Washington, 2024) for secure, anonymous tips, leveraging TOR to ensure anonymity and bidirectional security. Its success demonstrates TOR's viability as a sensitive reporting system.

RECOMMENDATIONS

To address the gap, and based on the best practices summarized above, the U.S. Government should implement a TOR-based anonymous reporting system combined with SecureDrop. Key features of this system include:

- **High Anonymity**: Non-attributable submissions through TOR (Salvo, 2021).
- **Robust Security**: Encryption to protect data in transit and at rest (Javed MS, 2024).
- **Optional Identity Features**: Allow users to share limited identifying details if desired, akin to The Washington Post's SecureDrop implementation.

IMPLEMENTATION CONSIDERATIONS

Key considerations for decision makers identified by the authors include the following:

- **Agency Leadership**: CISA and U.S. Cyber Command are well-suited for this initiative:
- **CISA**: Has the mandate (Security, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 2024) and infrastructure to operationalize a secure reporting platform quickly but would require interagency coordination for effective routing.
- **U.S. Cyber Command**: Its broad cybersecurity defense authority positions it as a potential lead organization.
- **Interagency Collaboration**: Ensuring seamless information sharing between agencies is critical for success.

CONCLUSION

The absence of a centralized, secure, and anonymous reporting mechanism for cyber threats undermines U.S. national security. A TOR-based reporting system would address this vulnerability, empowering individuals to report incidents without fear and enhancing intelligence-gathering efforts. By implementing this system within a capable agency, the U.S. Government can strengthen its cybersecurity defenses, foster greater trust in the intelligence community, and improve its resilience against cyber threats.

This initiative is essential to securing the nation's critical infrastructure and ensuring a robust defense against evolving cyber challenges.

ACKNOWLEDGEMENTS

The Institute of National Security acknowledges the support of the Vanderbilt University Office of the Provost through Discovery Vanderbilt initiative as well as the Office of the Chancellor, the School of Engineering, College of Arts & Sciences, and Peabody School of Education for their collaboration and support. The Institute also thanks our generous donors for investing in the professional development of the next generation of U.S. national security professionals.

REFERENCES

Advisers, T. C. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy.* Washington, D.C.: Executive Office of the President of the United States.

IBM. (2024). *Cost of Data Breach Report.* Armonk, NY: IBM Corporation.

Javed MS, S. S. (2024). Analyzing Tor Browser Artifacts for Enhanced Web Forensics, Anonymity, Cybersecurity, and Privacy in Windows-Based Systems. *Information*, 15(8):495.

Office, G. A. (2023, June 20). *Cybercrime: Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics*. Retrieved from GAO Products: https://www.gao.gov/products/gao-23-106080

Romanosky, S. (2016). Examining the costs and the causes of cyber incidents. *Journal of Cybersecurity, Volume 2, Issue 2*, 121-135.

Salvo, P. D. (2021). Securing Whistleblowing in the Digital Age: SecureDrop and the Changing Journalistic Practices for Source Protections. *Digital Journalism*, 443-460.

Schwartz, S. (2022, January 14). *Cybersecurity Dive Brief*. Retrieved from Cybersecurity Dive: https://www.cybersecuritydive.com/news/fbi-cisa-incident-response/617193/

Security, D. o. (2023). *Harmonization of Cyber Incident Reporting to the Federal Government.* Washington, D.C.: Department of Homeland Security Office of Strategy, Policy, and Plans.

Security, D. o. (2024, April 4). *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*. Retrieved from Federal Register: https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

Washington, A. (2024). *ACLU Washington*. Retrieved from ACLU of Washington's SecureDrop Risk Analysis: https://www.aclu-wa.org/aclu-washington-s-securedrop-risk-analysis

White, K. H. (2012). Information sharing requirements and framework needed for community cyber incident detection and response,. *2012 IEEE Conference on Technologies for Homeland Security (HST)* (pp. 463-469). Waltham, MA: IEEE.