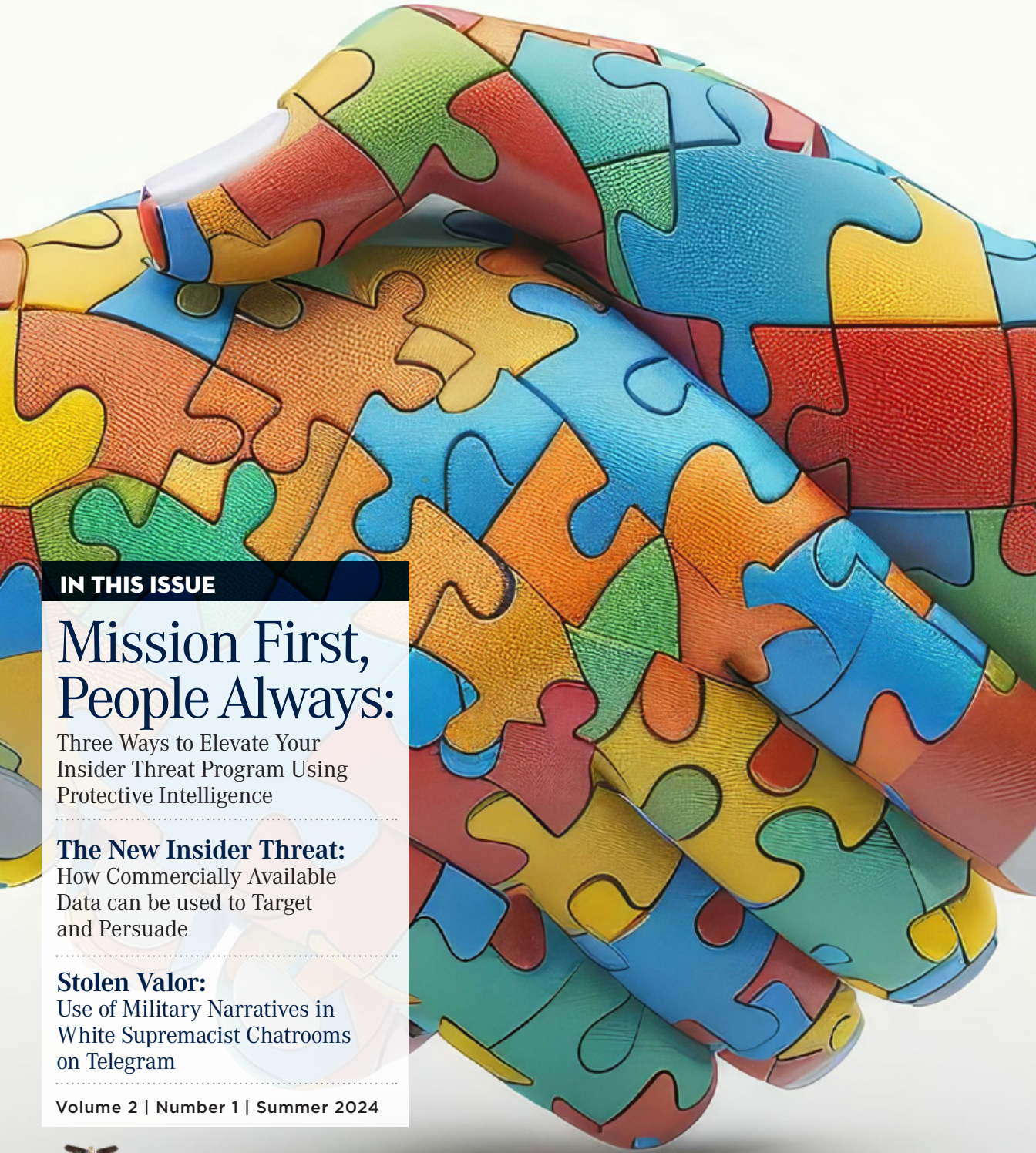
The MIROR JOURNAL

Managing Insider Risk and Organizational Resilience



IN THIS ISSUE

Mission First, People Always:

Three Ways to Elevate Your Insider Threat Program Using Protective Intelligence

The New Insider Threat:
How Commercially Available Data can be used to Target and Persuade

Stolen Valor:
Use of Military Narratives in White Supremacist Chatrooms on Telegram

Volume 2 | Number 1 | Summer 2024

WEST POINT PRESS

The Department of Defense Insider Threat Program

The Department of Defense (DoD) Insider Threat Program leads DoD efforts to prevent, deter, detect, and mitigate insider threats to the DoD enterprise.

Located within the Office of the Under Secretary of Defense for Intelligence and Security, Counterintelligence, Law Enforcement, and Security (OUSD (I&S), (CLS), the program provides governance and advocacy for insider threat programs across the DoD Components and Services supporting nearly 15 million personnel.

The program is dedicated to the pursuit of advanced capabilities integrated within DoD security reform and vetting efforts, and to the development of a well-equipped, trained, and vigilant workforce to protect DoD resources, personnel, installations, and other equities from insider threats.

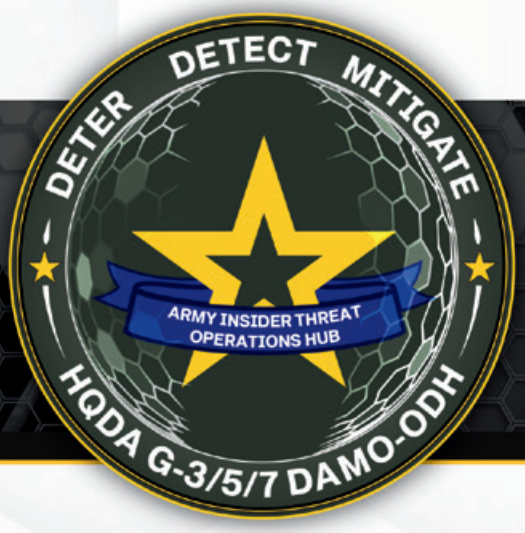
The DoD Insider Threat Program provides strategic oversight, issues policy and implementation guidance, and advocates for resources for the DoD Insider Threat community.

The office has played a critical role in advancing the mission through targeted investments in training and workforce professionalization and in advanced social and behavioral science research. The program also facilitates information sharing, collaboration, and continuous improvement of the insider threat discipline for stakeholders across the U.S. government and key partners in critical infrastructure.

For more information contact the OUSD(I&S) InT team's organizational box

osd.pentagon.ousd-intel-sec.mbx.dodcounterinsiderthreat@mail.mil

The U.S. Army Insider Threat Operations Hub is the operational element of the Counter-Insider Threat Program. It is designed to detect concerning behaviors from Army personnel and to deter, prevent, and mitigate threats to Army personnel, resources, and information.



The Hub utilizes Artificial Intelligence, Machine Learning, and other computer aided tools to identify behavioral patterns that may indicate an individual poses a risk to the Army.

Analysts compile information and consult with subject matter experts to assess risk and develop mitigation strategies.

The Hub further coordinates with "spoke" elements, including law enforcement, counter-intelligence, and security to ensure synchronized detection and response. We are proud to be the Army's first-line in detecting threats from within.

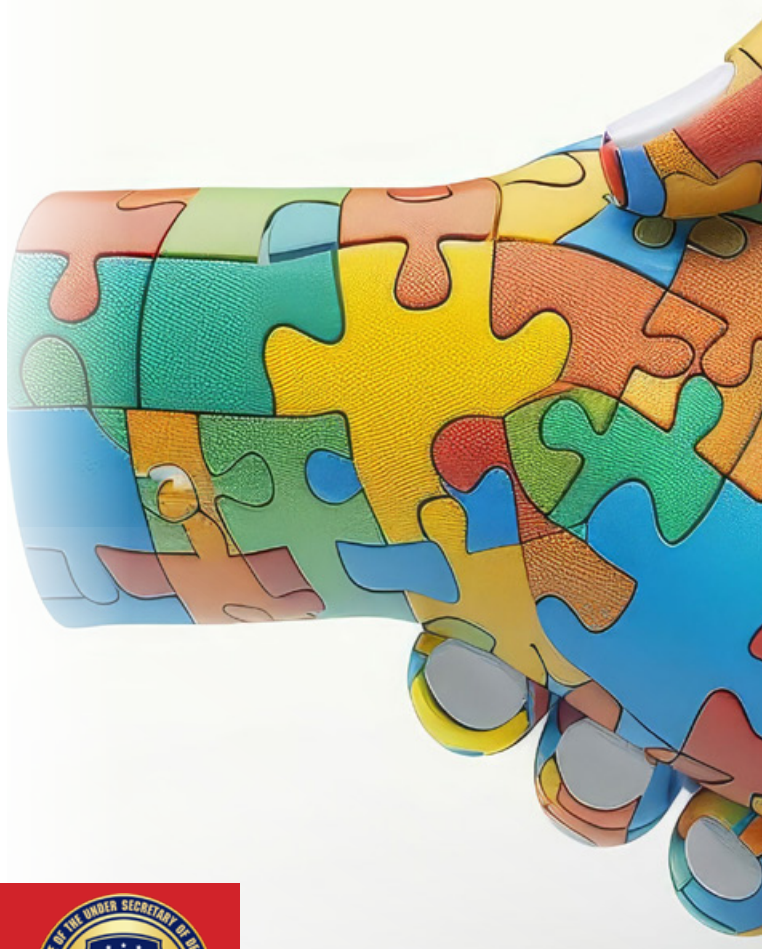
For questions or more information about the Hub, or to report concerning behavior, please contact:

usarmy.pentagon.hqda-dcs.mbx.g-34-int-hub-reports-cell@army.mil.

The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience

The Managing Insider Risk and Organizational Resilience (MIROR) Journal

Produced and edited by the West Point Insider Threat Program
Published by West Point Press



FUNDING FOR THE MIROR JOURNAL

Provided by the Defense Counterintelligence and Security Agency, DCSA, and Undersecretary of Defense for Intelligence & Security, USD(I&S).

The West Point Press is the publishing arm of the US Military Academy, producing scholarly content for students, scholars, and leaders.

Our scholarly books, digital textbooks, journals, and other content reflect a commitment to the highest standards of scholarship.

WEST POINT PRESS

ABOUT

The Managing Insider Risk & Organizational Resilience (MIROR) Journal (Online ISSN 2832-5427 Print ISSN 2832-5419) is a scholarly Open Access journal published by the West Point Press, the publishing arm of the United States Military Academy, and produced by the Insider Threat Research Research Program at the Department of Mathematical Sciences at the United States Military Academy. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute an endorsement by the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

COPYRIGHT

OPEN ACCESS STATEMENT

Managing Insider Risk & Organizational Resilience (MIROR) Journal is an Open Access Journal which means that all content is freely available without charge to the user or his/her institution. Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the articles, or use them for any other lawful purpose, without asking prior permission from the publisher or the author. This is in accordance with the Budapest Open Access Initiative (BOAI) definition of open access.

The Managing Insider Risk & Organizational Resilience (MIROR) Journal does not charge authors for submission, processing, and publication.

REPOSITORY POLICY

Managing Insider Risk & Organizational Resilience (MIROR) Journal is an Open Access journal and supports the author's self-archiving their manuscripts/articles on their personal or institutional website, university, specialized repositories such as ArXiv.org, and research sharing websites such as ResearchGate. Authors are allowed to deposit their works after it has been published in the Managing Insider Risk & Organizational Resilience (MIROR) Journal, either online or in print, with no embargo. Authors can publish submitted, accepted, published manuscript/article, or publisher's PDFs.

ARCHIVING POLICY

Managing Insider Risk & Organizational Resilience (MIROR) Journal allows anyone to archive the content. The MIROR Journal will ensure long-term open access to the content by uploading the content to the Department of Defense digital repository DTIC (Defense Technical Information Center) DoDTechipedia public collections, Internet Archive (Archive.org), and deliver the printed journal to the Library of Congress.

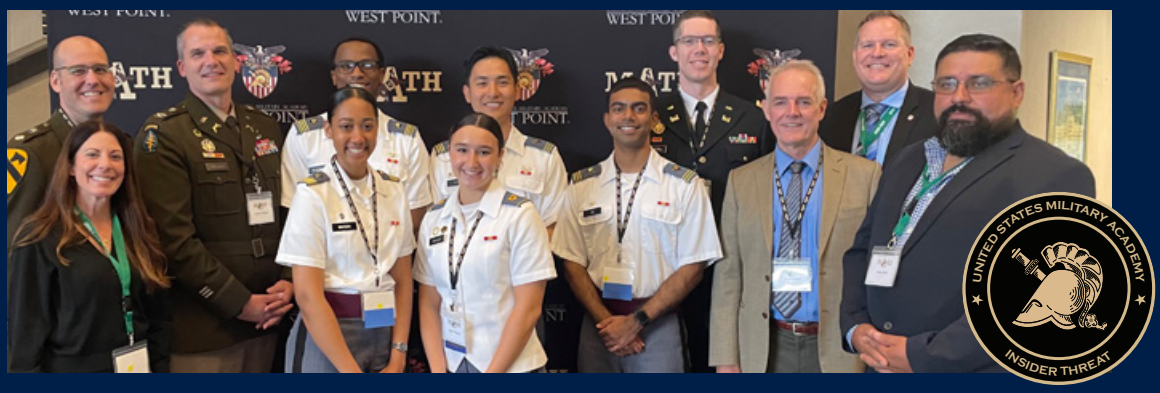
The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience
Volume 2 | Number 1 | Summer 2024

WELCOME

A SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

The West Point Insider Threat research team at the 2024 Math Research Symposium (MaRS)



Front row: MAJ Carrie Donoho (Research Facilitation Lab); PhD, Cadets Sydney Watson and Kayla Teuscher; Dr. Pedro Wolf (RFL)
Second: LTC Russell Nelson, PhD; COL Joseph Lindquist, PhD; Cadets Joshua Blackmon, Samin Kim, Saleem Ali; Dr. Charles Hogue (Uniformed Services University for the Health Sciences)
Back: MAJ Hayden Deverill and LTC(ret) Jon Roginski, PhD

The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience

Volume 2 | Number 1 | Summer 2024

ORIGINAL RESEARCH

LESSONS LEARNED AND CASE STUDIES

SUBMISSIONS AND CALL FOR PAPERS

WELCOME

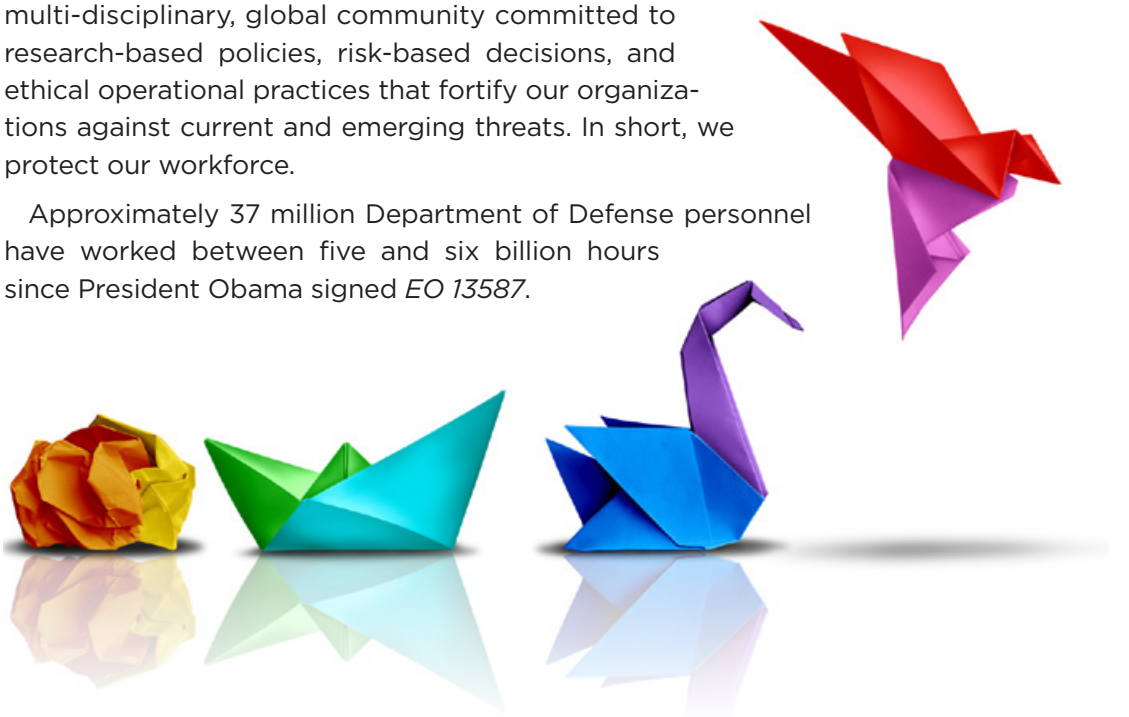
Workforce Protection: The Next Generation of Insider Risk Programs

Stephanie L. Jaros
Applied Research Laboratory for Intelligence and Security (ARLIS)
at the University of Maryland

Jonathan W. Roginski
United States Military Academy at West Point

Since 2011, our community has successfully transformed Insider Threat Programs from reactive, often collateral duty assignments into a critical mission area focused on prevention, wellness, and collaboration. Along the way we have established a professionalization roadmap that includes a global certification and a graduate certificate, and we have educated our colleagues, supervisors, and agency leaders. Today, in 2024, insider risk professionals are members of a multi-disciplinary, global community committed to research-based policies, risk-based decisions, and ethical operational practices that fortify our organizations against current and emerging threats. In short, we protect our workforce.

Approximately 37 million Department of Defense personnel have worked between five and six billion hours since President Obama signed *EO 13587*.



> **Workforce Protection...accurately represents the work that we are doing...it summarizes our approach to risk management...**

Fortunately, during this same period, we experienced and recovered from only a small number of high-impact insider threat events. Rare events present several programmatic and measurement challenges, and so in recognition of this reality, Insider Threat Programs moved away from predictive threat models toward risk management practices, and several groups relaunched as Insider Risk Programs.

While this change marked a meaningful step, it is not enough. "Insider Risk" still implies that risk resides only within the individual and suggests that if we remove the person from our agency, we remove the risk. This is not how we measure success. "Insider Risk" ignores the organizational factors that we know contribute to concerning behaviors that persist even as employees come and go. Also, it continues to evoke thoughts of constant surveillance and confrontation. "Workforce Protection," in contrast, accurately represents the work that we are doing in our Hubs. It summarizes our approach to risk management, which includes our efforts to identify and mitigate both individual and organizational issues, and our attention to the full career life cycle. We believe this change once again will move our mission and our community forward because it captures our holistic approach and hopefully, inspires continued innovation.

Stephanie L. Jaros
Visiting Research Scientist & Insider Risk Consultant
sjaros@arlis.umd.edu
Follow me on LinkedIn

LTC (ret) Jonathan W. Roginski, Ph.D.
Program Manager, Insider Threat
jonathan.roginski@westpoint.edu
Follow me on LinkedIn

DISCLAIMER

The information and views expressed in this presentation are solely those of the author and do not represent opinions and policies of the Department of Defense, U.S. Government, U.S. Special Operations Command, the Joint Special Operations University, or the institutions with which the author is affiliated.