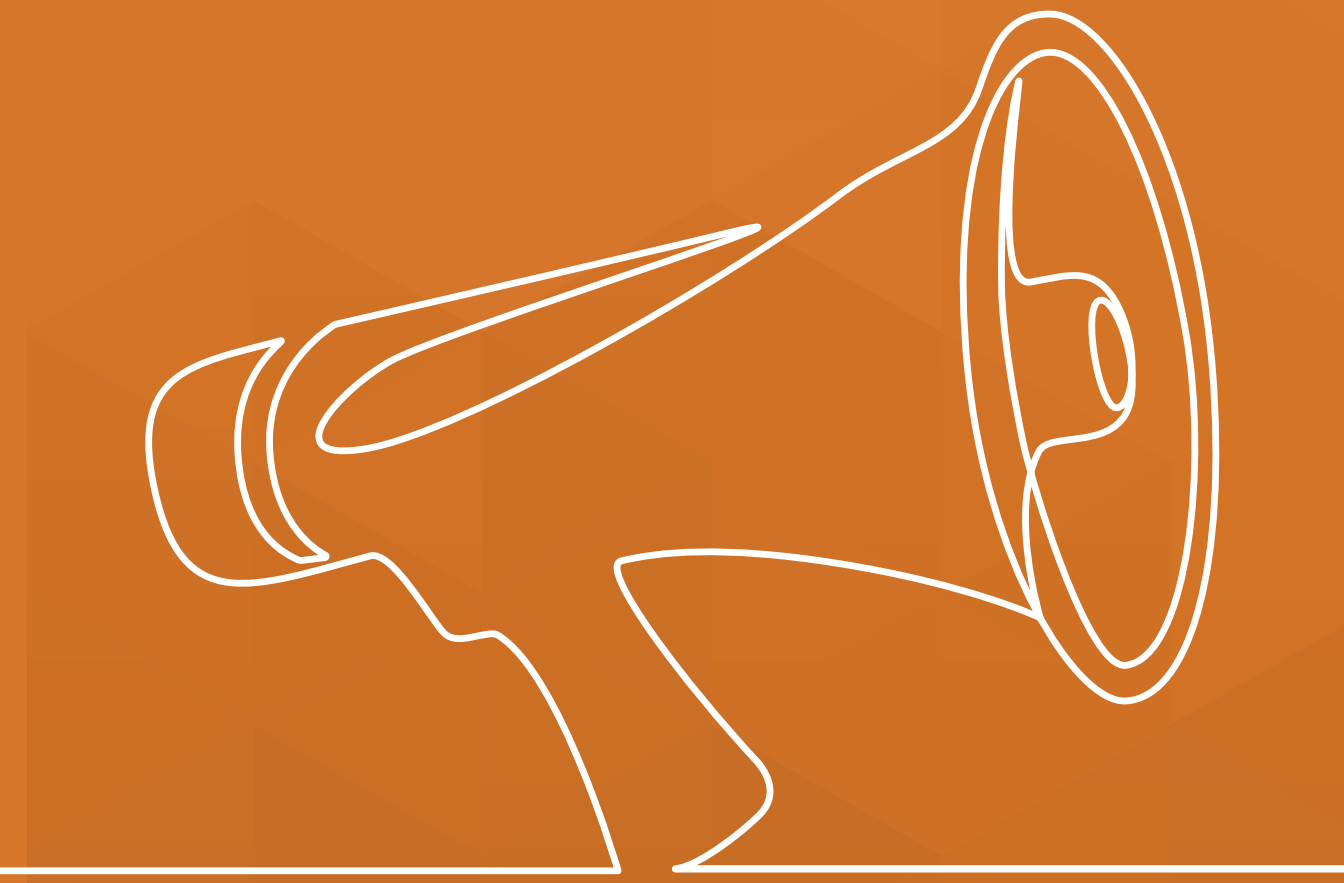

SUBMISSIONS AND CALL FOR PAPERS

Submissions and Call for papers

The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience

EDITOR-IN-CHIEF
Jonathan W. Roginski, Ph.D.

CONTACT
jonathan.roginski@westpoint.edu
insiderthreat@westpoint.edu

MANUSCRIPT SUBMISSIONS
https://www.editorialmanager.com/mirorjournal/default2.aspx

Managing Insider Risk and Organizational Resilience (MIROR) Journal is an editorial-reviewed online and print publication. MIROR will share research, best operational practices, leadership perspectives, and reviews of relevant work that further both the proactive practices of insider risk management and promotion of holistic wellness and resilience in organizations.

The editors will review content across those areas that move discussion forward concerning insider risk and organizational resilience, including but not limited to the following:

- **Recruitment and pre-employment screening.** How do we recruit and hire the right "fit" for our organization, facilitating higher performance and better retention?
- **Development and/or implementation of policies and practices.** How does an agency build policies and practices to accomplish its mission while maximally protecting against risks presented to mission accomplishment from the inside?
- **Training and education.** How do we effectively train the workforce on policies and practices (prepare for the known) and educate toward continuous improvement (prepare for the unknown)?
- **Continuous evaluation.** How do we foster trust across the enterprise by thoughtfully and respectfully verifying the alignment of values between individual and organization extant at hiring continues to result in mutually supportive behaviors?

- **Risk modeling and reporting.** How do we leverage the suite of quantitative and qualitative mathematical, statistical, and mental models that exist (or will exist) against the challenge of keeping people and organizations happy, healthy, and safe? How are the results of those models communicated to leaders to facilitate decision making and change?
- **Data science applications.** Data science is arguably the most "in-demand" contemporary analytical field—how may we benefit from the groundbreaking knowledge and techniques in the insider risk and threat management field?
- **Creation and maintenance of positive organizational culture.** Employees that are connected to and invested in their organization and feel reciprocity from the company are protective and constructive toward themselves, their peers, and the company. How do we make, keep, and foster such an environment?
- **Employee intervention.** Identify people and practices that increase risk of negative insider activity and align appropriate resources to protect people and the enterprise?

ARTICLE TYPES AND SUBMISSION

Submissions in the following categories are welcome:

Professional Commentary (800+ words) Professional commentaries seek to bring forward insight from leaders in the field and highlight recent developments, concerns, and bridge gaps between industry, government, and academia. A Professional Commentary includes references as embedded discussions in the text and no endnotes.

Traditional Research Article (up to 5,000 words) with findings and results.

Research Notes are short articles (1500 – 2500 words) with preliminary findings, early results, or responses to current developments. Endnotes must be hyperlinked with the text referenced. Discursive endnotes are strongly discouraged; cite only direct quotations and paraphrases. No need for a bibliography. The journal's formatting style is the Chicago Manual of Style (CMS), 17th edition, endnotes.

Lessons Learned, Case Studies, Vignettes (500 – 1500 words) Experiences from practitioners and professionals close to the developments in the field. The article type is a feedback loop from the field back to the community. A Lessons Learned, Case Studies, Vignettes article has needed references as embedded discussions in the text and no endnotes.

Review Article (1000 – 2000 words) Synthesize seminal and/or canonical works in a particular area informing the ideas of insider risk and organizational resilience to inform the readership of important foundational knowledge in the field.

Book Review (1000 words) Traditional academic book review with no endnote references.

The HQDA G-3/5/7, DAMO-ODP, Army Counter-Insider Threat Program is an integrated effort across the Total Army established to protect installations, networks, facilities, personnel, and missions from the risk insiders pose to national security.

U.S. ARMY

COUNTER-INSIDER THREAT PROGRAM

HQDA | DCS | G-3/5/7 | DAMO-ODP/DAMO-ODH

From the offsite contractor logically accessing Army networks to the senior Army leader stationed on the Pentagon Reserve, and Soldiers, staff, and personnel everywhere in between, the Army Counter-Insider Threat Program develops policies and procedures to improve the Army's reaction and pre-emptive responses to combat risks posed by existing and evolving threats.

The **Army Counter-Insider Threat Program Management Team** consists of highly trained individuals focused on policy development training and awareness, reporting procedures, and data processing to continually enable all Army Commands, Army Service Component Commands, and Direct Reporting Units to prevent, deter, detect, and mitigate insider threats.

For questions or for more information about the Army Counter-Insider Threat Program please contact the organizational inbox:

usarmy.pentagon.hqda-dcs-g-3-5-7.mbx.damo-odp-counter-int@army.mil.

the ThreatLab

Integrating Research Into Practice

The insider threat is a human problem resulting from a complex interaction among individuals and environmental factors.

Social and behavioral sciences are well-suited to address this complicated and persistent human problem.

The Defense Personnel and Security Research Center founded the Threat Lab in 2018 to incorporate the social and behavioral sciences into the counter-insider threat mission space. Our vision is to be a global leader in creating and sharing social and behavioral sciences knowledge to counter the insider threat.

- We work with stakeholders to transform operational challenges into actionable research questions.
- We design and execute research projects that result in accessible, concise findings and recommendations
- We integrate into training and awareness materials that organizations can use or customize for their own purposes.

The Threat Lab portfolio includes exploratory research, professionalization (education, training, certification and tradecraft programs) and outreach activities.

The West Point Insider Threat Program connects Department of Defense and Department of the Army's Insider Threat efforts with an interdisciplinary team to counter insider threat by fostering a positive leadership climate that reduces threat likelihood and impact.

When the Office of the Under Secretary of Defense (I&S) and the Department of Army recognized a need; the US Military Academy and Department of Mathematical Science answered the call. The result is the Insider Threat Program which builds an ecosystem of trust, development, and caring to create an environment incompatible with Insider or Inside Threat.

Change the conversation about Insider Threat

- Why does Insider Threat happen?
- How do we prevent?
- How do we detect?
- How do we mitigate effects?

Support to DoD and Army

- Oath to Constitution
- Army Prioritized Protection List
- Network Engagement Team

Deploy Artifacts

- Undergraduate internships, presentations, theses
- MIROR Journal

For inquiries and information about West Point Insider Threat Program
email: insiderthreat@westpoint.edu
web: insiderthreat.westpoint.edu

The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience