Opportunity Title: Minimizing Time to Recovery While Maximizing Architectural Agility in Cyber Systems
Opportunity Reference Code: ICPD-2025-27

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2025-27

How to Apply **Create and release your Profile on Zintellect** – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 3 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orise.orau.gov/icpostdoc/index.html.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline 2/28/2025 6:00:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

The dangers and costs of a successful cyberattack1 are increasing and evolving, particularly in relation to ransomware and the threat of data exfiltration for extortion resulting from intrusions. A successful strategy for recovering from cyberattacks requires a dedicated secure isolated recovery environment (SIRE), but there remains no single, set blueprint for how a SIRE should be designed.

When developing SIREs, industry focus appears to be on data backups. How should this pattern best be applied when the primary restoration target is functionality, instead of data? Consider an information processing environment, where long-term data storage is handled outside the system boundary. A key requirement of this system is that it be adaptable and allow for rapid architectural change as processing needs evolve. Short of replicating the entire environment, what options exist for the implementation of a SIRE to speed time to recovery (TTR)? Is TTR orthogonal to system agility?

Example Approaches:

The NIC must design and build system recovery mechanisms as part of an overall cyber recovery strategy for mission-critical systems. The focus must be on optimizing this backup infrastructure to ensure that the organization can restore functionality after an incident, and that disruption to business activities is managed according to valid and up to date plan.

1. Have we identified important NIC data holdings and data processing dependencies to support our armed forces in case of regional conflict or escalation?
2. How can isolated recovery environments be kept in-sync with rapidly changing systems, while maintaining an effective security boundary?

3. Are we understating or overestimating the possibility of a direct attack on NIC air-gapped systems and infrastructure? Why should we be comfortable with the existing system recovery and data restoration arrangements?
4. What infrastructure is required for system recovery and data restoration? Can open-source efforts towards software supply chain security be leveraged to build confidence in a path to restoration?

Relevance to the Intelligence Community:

While data is the lifeblood of the National Intelligence Community (NIC), functions like secure communication and intelligence collection are typically separate from data storage and processing. Recovering these systems from an incident or attack may require different approaches. The NIC's existing strategy relies heavily on.

Determined cybercriminal and/or espionage adversaries may use unconventional methods to infiltrate air gapped systems— researchers from Israel's Ben-Gurion University of the Negev and Shamoun College of Engineering [1] demonstrated how this could be done. They created a malware that could "bridge" air-gapped systems via the electromagnetic capabilities in of compromised surveillance cameras.

Given these methods exist, the NIC must constantly assess what levels of isolation are appropriate. Increasing system inter-connection can lead to efficiencies and agility but may come at the cost of recoverability. In the other direction, strong isolation runs the risk of environmental drift. Striking the right balance will be critical to ensuring the ongoing ability of the NIC to deliver on its commitments to government.

References:

[1] This evasive new cyberattack can bypass air-gapped systems to steal data from the most sensitive networks | ZDNET, https://www.zdnet.com/article/this-evasive-new-cyberattack-can-bypass-air-gapped-systems-to-steal-data-from-the-most┐ sensitive-networks/

Key Words: Cybersecurity, resilience, availability, agility, information assurance, SIRE, ransomware, cyber-attack, intrusion.

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the appointment start date
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Point of Contact Keri Tarwater

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (3 👁)
  - **Computer, Information, and Data Sciences** (17 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (11 👁)
  - **Other Non-Science & Engineering** (2 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (30 👁)