Journal of Management Information Systems
Special Section on Critical National Infrastructure

Due Date: January 31, 2026

Guest Editors of the Special Section

- Jason Chan (jchancf@umn.edu), University of Minnesota
- Alan Dennis (ardennis@iu.edu), Indiana University
- Daniel Gozman (daniel.gozman@sydney.edu.au), The University of Sydney
- Kalle Lyytinen (kalle@case.edu), Case Western Reserve University

Background:

Critical National Infrastructure (CNI) encompasses essential systems and services that are vital for societal stability, economic security, and national safety. The increasing digitalization of these infrastructures has introduced unprecedented efficiencies that have transformed economies (Gao and Lyytinen, 2005), enabling faster service delivery, improved public safety, reduce corruption and enhanced crisis response through data sharing and analytics (Sarker et al., 2021). The United Nations Development Programme (UNDP) supports digital public infrastructure (DPI) as a driver for financial inclusion, social protection, and governance reforms. Digital advancements have also driven sustainability, with smart grids (Piel et al., 2017), environmental monitoring, and optimized resource management with potential for reducing carbon footprints and increasing resilience. Furthermore, technological innovation in financial services, transportation, and energy has the potential to stimulate economic growth through enabling new business models.

While the increasing digitalization of Critical National Infrastructure has introduced efficiencies it also created unprecedented vulnerabilities, including cyberattacks, cascading failures, and systemic interdependencies that amplify risks (Plachkinova & Vo, 2023; August, Dao & Niculescu, 2022). Recognizing these challenges, governments in the UK, US, and Australia have developed regulatory frameworks such as the UK's National Cyber Security Strategy, the US Cybersecurity and Infrastructure Security Agency (CISA) guidelines, and Australia's Security of Critical Infrastructure Act (SOCI Act) to enhance resilience and mitigate emerging threats. CNI spans multiple critical sectors, each with unique security and operational challenges, including energy and utilities (Milosevic, Bass, and Combs, 2018), telecommunications and information networks (Lips et al., 2023), financial services and payments (August, Dao, and Niculescu, 2022), healthcare and public health (Sakurai & Chughtai, 2020), transportation and logistics (Guo, Liu, and Nault, 2024), emergency services and law enforcement (Schakel, van Fenema, and Faraj, 2016), and government and public sector infrastructure (Plachkinova & Vo, 2023). As efforts to build CNIs have accelerated, issues around CNI security, resilience, and adaptability are becoming increasingly critical. At the same time significant research gaps remain in cybersecurity practices at the system level, governance, integration and management of emerging technologies such as Autonomous Driving Systems[1], and threat intelligence sharing. Addressing these gaps is essential for policymakers, businesses, and infrastructure operators to mitigate threats, optimize performance, and ensure long-term continuity (Sakurai & Chughtai, 2020; Lips et al., 2023).

This Special Section aims to advance research on the design, adoption, and impact of digital solutions and services critical in building CNI to enhance governance, economic development, and public service delivery and safeguard CNI. We invite interdisciplinary contributions that explore how digital technologies and services can enhance CNI or impose new risks and challenges for the operation of CNIs. Papers that do not explicitly address or theorize about CNI design and operation and their digital components will be returned without review. For

[1] Recent Netflix series Zero Day shows the potential impacts and challenges in addressing such risks.

example, papers focused on digital transformation at industry level or on cybersecurity presenting models applicable to a wide variety of application contexts while fail to consider the unique context of CNI, will not be considered.

Suggested topics include but not limited to the following:

1. Emerging Technologies and Digital Transformation
Innovative technologies such as Artificial Intelligence, Digital Twins (Lyytinen et al., 2023), Blockchain and IoT are transforming CNI (Chen et al., 2024), enabling predictive analytics, smart grids, and cyber-physical security enhancements. Digital transformation plays a crucial role in digitizing critical infrastructures (Poláková-Kersten et al., 2023), enhancing operational efficiency, and enabling new service models, particularly in sectors such as healthcare, where digital complementary assets are key drivers of innovation (Steinhauser, Doblinger, and Hüsig, 2020).

2. Cybersecurity, Resilience, and Risk Management
CNI becomes increasingly interconnected, cyber threats such as ransomware, insider attacks, and cyber-physical vulnerabilities continue to grow (Plachkinova & Vo, 2023, Kumar, Marston & Sen, 2020). Risk assessment frameworks and mitigation strategies are essential to protect infrastructure while addressing the economic impact of breaches and strengthening cybersecurity policies (August, Dao & Niculescu, 2022; Hui, Hui, and Yue, 2012; Salovaara, Lyytinen, and Penttinen, 2019). Additionally, CNI resilience depends on anticipating, withstanding, and recovering from disruptions, as seen in past disasters and cyber incidents (Sakurai & Chughtai, 2020; Rezazade Mehrizi, Nicolini & Mòdol, 2022). Strengthening CNI security and resilience demands a proactive, integrated approach to risk management, business continuity, and information sharing (Zhuang et al., 2020; Kolini & Janczewski, 2022).

3. Governance, Policy, and Public-Private Partnerships
CNI governance requires polycentric collaborative efforts between government agencies, private sector entities, and international stakeholders (Guo, Liu & Nault, 2024). The governance is an mix of public-private partnerships influencing the management of national infrastructure (Lips et al., 2023). Effective governance frameworks ensure that policy, compliance, and regulatory mechanisms align with evolving security challenges (Hassandoust and Johnston, 2023). Governance frameworks for payments, identity management, and data sharing play a crucial role in securing financial and digital infrastructures.

We welcome research using diverse methodologies and approaches, including:

- **Qualitative** (e.g., case studies, interview-based, ethnographic studies)
- **Quantitative** (e.g., experiments, econometric modelling, survey-based)
- **Design science** (e.g., development and evaluation of artifacts)

Timeline:
Authors should submit a one-page extended abstract to the Guest Editors prior to submission to assess the fit of their paper with the special section. The abstract should clearly present the research question, theory, method and expected contribution. Authors are encouraged to submit prior to the deadline and papers will be processed as they are received. The editorial timeline will proceed as follows:

- **Expression of Interest**: June 1, 2025 (one-page abstract, **optional**) to jmiscni@gmail.com
- **Initial Submission Due:** January 31, 2026 to jmiscni@gmail.com
- **Notification of First Round Decision:** May 31, 2026
- **1st Resubmission Due:** September 30, 2026
- **Notification of Second Round Decision:** January 31, 2027
- **2nd Resubmission Due:** April 30, 2027
- **Final Decision:** June 15, 2027

References:

August, T.; Dao, D.; and Niculescu, M.F. Economics of ransomware: Risk interdependence and large-scale attacks. *Management Science*, 68, 12 (2022), 8879-9002.

Chen, Y.; Lu, Y.; Bulysheva, L.; and Kataev, M.Y. Applications of blockchain in Industry 4.0: A review. *Information Systems Frontiers*, 26, 5 (2024), 1715-1729.

Gao, P.; and Lyytinen, K. Formulating effective national strategies for market transformation. *Journal of Information Technology*, 20, 3 (2005), 201-210.

Guo, H.; Liu, Y.; and Nault, B.R. Join up or stay away? Coalition formation for critical IT infrastructure. *Information Systems Research*, 35, 3 (2024), 1344-1362.

Hassandoust, F.; and Johnston, A.C. Peering through the lens of high-reliability theory: A competencies-driven security culture model of high-reliability organisations. *Information Systems Journal*, 33, 5 (2023), 1212-1238.

Hui, K.L.; Hui, W.; and Yue, W. Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems*, 29, 3 (2012), 117-156.

Kolini, F.; and Janczewski, L. Exploring incentives and challenges for cybersecurity intelligence sharing (CIS) across organizations: A systematic review. *Communications of the Association for Information Systems*, 50, 1 (2022), 86-121.

Kumar, C.; Marston, S.; and Sen, R. Cyber-physical systems (CPS) security: State of the art and research opportunities for information systems academics. *Communications of the Association for Information Systems*, 47, 1 (2020), 678-696.

Lips, S.; Tsap, V.; Bharosa, N.; Krimmer, R.; Tammet, T.; and Draheim, D. Management of national eID infrastructure as a state-critical asset and public-private partnership: Learning from the case of Estonia. *Information Systems Frontiers*, 25, 6 (2023), 2439-2456.

Lyytinen, K.; Weber, B.; Becker, M.C.; and Pentland, B.T. Digital twins of organization: implications for organization design. *Journal of Organization Design*, 13 (2023), 77-93.

Milosevic, I.; Bass, A.E.; and Combs, G.M. The paradox of knowledge creation in a high-reliability organization: A case study. *Journal of Management*, 44, 3 (2018), 1174-1201.

Piel, J.-H.; Hamann, J.F.H.; Koukal, A.; and Breitner, M.H. Promoting the system integration of renewable energies: Toward a decision support system for incentivizing spatially diversified deployment. *Journal of Management Information Systems*, 34, 4 (2017), 994-1022.

Plachkinova, M.; and Vo, A. A taxonomy for risk assessment of cyberattacks on critical infrastructure (TRACI). *Communications of the Association for Information Systems*, 52 (2023), 1-25.

Poláková-Kersten, M.; Khanagha, S.; van den Hooff, B.; and Khapova, S.N. Digital transformation in high-reliability organizations: A longitudinal study of the micro-foundations of failure. *Journal of Strategic Information Systems*, 32, 1 (2023), 101756.

Rezazade Mehrizi, M.H.; Nicolini, D.; and Mòdol, J.R. How do organizations learn from information system incidents? A synthesis of the past, present, and future. *MIS Quarterly*, 46, 1 (2022), 531-590.

Sakurai, M.; and Chughtai, H. Resilience against crises: COVID-19 and lessons from natural disasters. *European Journal of Information Systems*, 29, 5 (2020), 585-594.

Salovaara, A.; Lyytinen, K.; and Penttinen, E. High reliability in digital organizing: Mindlessness, the frame problem, and digital operations. *MIS Quarterly*, 43, 2 (2019), 555-578.

Sarker, S.; Henningsson, S.; Jensen, T.; and Hedman, J. Use of blockchain as a resource for combating corruption in global shipping: An interpretive case study. *Journal of Management Information Systems*, 38, 2 (2021), 338-373.

Steinhauser, S.; Doblinger, C.; and Hüsig, S. The relative role of digital complementary assets and regulation in discontinuous telemedicine innovation in European hospitals. *Journal of Management Information Systems*, 37, 4 (2020), 1155-1183.

Zhuang, Y.; Choi, Y.; He, S.; Leung, A.C.M.; Lee, G.M.; and Whinston, A. Understanding security vulnerability awareness, firm incentives, and ICT development in Pan-Asia. *Journal of Management Information Systems*, 37, 3 (2020), 668-693.