

Private Security Deployments in Critical National Infrastructure (CNI) and Foreign Assets in Uganda

Freeman Crispus¹, Amos Garindwa²

1 Metropolitan International University, 2 NSG Ndugari Security Group

Abstract

This study examined private security deployments in critical national infrastructure (CNI) and the protection of foreign assets in Uganda, focusing on governance frameworks, operational performance, and strategic security risks. CNI comprised essential infrastructure and services whose disruption could affect national security, economic activity, public safety, and service delivery. Uganda's expanding investments in energy, telecommunications, banking, transport, manufacturing, agribusiness, and public infrastructure had increased the number of strategically important assets requiring effective protection. Foreign assets, including multinational corporate facilities, diplomatic missions, telecommunications investments, financial institutions, oil and gas installations, and other foreign-owned properties, had similarly expanded alongside foreign direct investment. Against this background, the study assessed how PSO vetting, security-protocol compliance, intelligence sharing, and state coordination influenced threat detection, incident response, and protective security resilience. Descriptive statistics revealed significant gaps in CNI-specific security governance (means 2.94–3.47). All three governance dimensions were significantly correlated with CNI security effectiveness ($r = 0.583\text{--}0.748$, $p < .001$). The three dimensions collectively explained 65.2% of variance in CNI security effectiveness ($R^2 = 0.652$, $F = 41.87$, $p < .001$). SEM confirmed intelligence sharing and state coordination as the strongest total effect predictor (total $\beta = 0.521$), with CNI protocol compliance partially mediating this relationship. Recommendations address CNI security tiering legislation, intelligence coordination protocols, foreign asset security governance frameworks, and national CNI protection strategies.

Keywords: Critical National Infrastructure, Private Security, Foreign Assets, PSO, Intelligence Coordination, CNI Protection, Oil and Gas Security, Diplomatic Protection, SEM, Uganda

1.0 Background of the Study

Critical national infrastructure-the systems, facilities, and assets whose disruption or destruction would have severe consequences for public safety, national security, economic stability, or essential service continuity had in Uganda expanded dramatically in both scope and strategic importance over the preceding decade. The development of oil and gas production infrastructure in the Albertine Rift (including Total Energies', Tilenga project, CNOOC's, Kingfisher development, and the East African Crude Oil Pipeline connecting Kbaale Kibaale to Tanzania's Tanga Port), the expansion of telecommunications backbone infrastructure by MTN, Airtel, and Liquid Telecom, the growth of Uganda's banking sector to 26 licensed commercial banks with combined assets exceeding UGX 38 trillion, and the development of strategic government facilities including Entebbe International Airport's expanded cargo terminal collectively constituted a CNI portfolio whose aggregate economic and strategic value made its security a matter of national consequence extending well beyond the commercial interests of individual asset owners.

The protection of foreign assets in Uganda had added an important layer of diplomatic, commercial, and international governance complexity to the country's private security environment. Uganda hosted 41 foreign diplomatic missions, alongside foreign-owned and foreign-invested enterprises, multinational corporations, international organisations, financial institutions, telecommunications companies, oil and gas interests, construction firms, and other strategically significant foreign-linked assets. The protection of these assets involved not only Uganda's domestic regulatory requirements for private security organisations (PSOs), but also diplomatic obligations, international standards, contractual requirements of foreign investors, and security expectations established by foreign governments and multinational organisations. The increasing use of Ugandan PSOs to protect foreign-owned facilities and investments had therefore created an intersection between national security regulation, diplomatic security requirements, corporate risk-management standards, and international responsible-security principles. This evolving environment had also strengthened the role of the Uganda Private Security Association (TUPSA) in promoting professionalisation, training, certification, regulatory compliance, and alignment with international standards. TUPSA's collaboration with the International Code of Conduct Association (ICoCA) had supported capacity building among private security company directors and senior managers, including training on human rights, responsible security practices, workplace safety, and professional standards. TUPSA became an ICoCA Observer in January 2025, strengthening the sector's engagement with internationally recognised responsible-security practices. These developments demonstrated that the protection of foreign assets in Uganda increasingly depended on PSOs operating within both national regulatory requirements and internationally recognised standards of professional and responsible security provision. However, this overtime has been closed with the PSOs engaging in seeking international standards such as The International Law Framework for Private Security; - International Code of Conduct Association for Private Security Providers, ICoCA. And standardization of operations Quality to international demands. Standards like ISO 9001 (Quality Management), the PSOs in Uganda have got these certifications hence local and international agencies trust. The strategic risk dimension of CNI private security deployments was particularly acute in the context of Uganda's oil and gas development. The Albertine Rift's proximity to the Democratic Republic of Congo a country experiencing sustained armed group activity including the Allied Democratic Forces (ADF) operating near the Uganda border and to the South Sudan border where residual instability and population displacement created security challenges meant that PSOs deployed to protect oil production infrastructure operated in threat environments requiring military-grade risk assessment, intelligence integration, and incident response capabilities that most commercial PSOs were neither trained nor equipped to provide. The governance gap between what CNI security required and what Uganda's existing PSO regulatory framework demanded or monitored created strategic security vulnerabilities that this study systematically examined.

2.0 Problem Statement

Received: 14.09.2026

Accepted: 20.09.2026

Published on: 30.09.2026

Uganda's existing PSO regulatory framework-the Private Security Organizations Act (2002) and regulations (2009) established no CNI-specific security standards, no differentiated clearance requirements for personnel deployed to high-risk national infrastructure, no mandatory intelligence sharing protocols between PSOs and state security agencies at CNI sites, and no special inspection or audit regime for PSOs operating in strategic national security environments. This regulatory gap meant that PSOs protecting Uganda's most strategically significant assets were subject to identical oversight as those providing residential security services-a one-size-fits-all approach that leading international CNI protection frameworks, including the UK's Centre for the Protection of National Infrastructure (CPNI) standards and the United States Department of Homeland Security's Critical Infrastructure Protection (CIP) directives, had long identified as inadequate. The absence of CNI-specific PSO governance was a regulatory vulnerability with potentially severe national security consequences as Uganda's oil production commenced and as foreign asset portfolios expanded.

3.0 Main Objective

The main objective was to examine private security deployments in critical national infrastructure and foreign assets in Uganda. Specific objectives were: (i) to assess the influence of CNI-specific PSO vetting and clearance standards on CNI security effectiveness; (ii) to evaluate the effect of CNI security protocol compliance on incident response and protective security performance; and (iii) to determine the relationship between intelligence sharing and state coordination mechanisms on CNI security resilience outcomes.

4.0 Literature Review

4.1 Theoretical Framework

The study was anchored on the Nodal Governance Theory (Johnston & Shearing, 2003), which conceptualized contemporary security provision as a network of public and private nodes-state agencies, private security firms, intelligence services, and asset owners whose effective interconnection and coordination determined the quality of security outcomes, rather than attributing security provision exclusively to state actors. Applied to CNI security, the theory predicted that effectiveness was determined not by the quality of individual nodes (state security agencies or PSOs in isolation) but by the quality of coordination, information sharing, and role complementarity among all nodes in the CNI security network. Critical Infrastructure Protection Theory (Rinaldi et al., 2001) informed the specific analysis of CNI security effectiveness, identifying interdependency-the reciprocal operational relationships among CNI sectors as the key analytical concept: threats to one CNI sector cascaded through interdependencies to affect others, implying that CNI security governance needed to be networked and intelligence-integrated to manage cross-sectoral threat dynamics. The International Law Framework for Private Security (Montreux Document, 2008; International Code of Conduct Association for Private Security Providers, ICoCA 2010) provided the normative framework for evaluating PSO foreign asset deployments against international standards for private military and security company conduct in complex operational environments.

4.2 Empirical Literature

Received: 14.09.2026

Accepted: 20.09.2026

Published on: 30.09.2026

Research on private security deployments in CNI contexts across Africa had documented both the indispensable contribution of PSOs to infrastructure protection and the significant governance challenges of unregulated or under-regulated deployments. De Witte (2020) documented in a study of oil infrastructure security in Sub-Saharan Africa that PSOs without intelligence integration protocols with state security agencies missed an estimated 64% of advance threat indicators that state intelligence channels captured, creating security blind spots that adversarial actors exploited. Isima (2019) found in a study of Nigerian oil infrastructure security that PSOs with formalized Joint Operations Centres co-located with military and police liaison officers achieved incident response times 58% faster than those operating in isolation, confirming the operational significance of intelligence coordination mechanisms. In Uganda specifically, Tangri and Mwenda (2010) documented the emerging governance challenges of oil sector security as the Albertine Rift development commenced, identifying the absence of a CNI-specific security regulatory framework as the most acute governance gap in Uganda's oil sector security architecture.

5.0 Methodology

A cross-sectional mixed-methods design was employed. The study population comprised security managers and stakeholders at Uganda's primary CNI sites and foreign asset locations. Purposive sampling yielded 196 respondents: CNI site security managers (52), PSO operations directors with CNI contracts (44), state security liaison officials at CNI sites (38), foreign diplomatic mission security coordinators (24), asset protection officials from regulatory bodies (22), and independent security sector assessment experts (16). Cronbach's Alpha: CNI-specific vetting 0.87, CNI protocol compliance 0.84, intelligence sharing and coordination 0.86, CNI security effectiveness 0.89. SPSS 26 and AMOS 24 were used. Twelve key informant interviews and structured CNI site security assessments at four representative infrastructure locations provided qualitative triangulation.

6.0 Results

6.1 Descriptive Statistics

Table 1: Descriptive Statistics-CNI Security Governance Dimensions and Effectiveness (N = 196)

Variable	N	Min	Max	Mean	Std. Dev
CNI-Specific PSO Vetting & Clearance	196	1.00	5.00	2.94	1.04
CNI Security Protocol Compliance	196	1.00	5.00	3.21	0.98
Intelligence Sharing & State Coordination	196	1.00	5.00	3.47	0.91
CNI Security Effectiveness	196	1.00	5.00	3.18	0.94

Source: Primary Data, 2026

The descriptive results document a CNI security governance landscape characterized by significant deficits across the most foundational security standards dimensions and moderate performance on the intelligence and coordination dimension. CNI-specific PSO vetting and clearance received the lowest mean score (mean = 2.94, SD = 1.04), reflecting the near-complete absence of differentiated security clearance standards for PSO personnel deployed to strategic infrastructure — with most CNI-deployed PSOs applying identical vetting procedures to infrastructure

Received: 14.09.2026

Accepted: 20.09.2026

Published on: 30.09.2026

guards as to residential security guards, without enhanced criminal record checks, foreign travel scrutiny, financial vulnerability assessment, or counter-intelligence clearance review. The high standard deviation (1.04) indicated wide variability between PSOs, with some major CNI operators — particularly those in the oil and gas sector responding to international client security standards — implementing enhanced vetting, while smaller PSOs at lower-profile CNI sites applied only the minimum regulatory standard. CNI security protocol compliance received a moderate mean (mean = 3.21, SD = 0.98), reflecting partial implementation of CNI-specific security protocols including access control systems, perimeter security standards, and incident reporting procedures, with compliance quality strongly influenced by client specification requirements rather than regulatory mandates. Intelligence sharing and state coordination received the highest mean among the three governance dimensions (mean = 3.47, SD = 0.91), reflecting the relatively more developed practice of information exchange between PSO site commanders and Uganda Police, UPDF, and Internal Security Organization (ISO) liaison officers at major CNI sites — particularly in the Albertine oil region where military-PSO coordination arrangements had been developed under the Joint Operations Centre model. Overall CNI security effectiveness received a mean of 3.18 (SD = 0.94), indicating moderate and highly variable security effectiveness across Uganda's CNI portfolio.

6.2 Correlation Analysis

Table 2: Pearson Correlation Matrix: CNI Security Governance and Effectiveness (N = 196)

Variable	1	2	3	4
1. CNI-Specific Vetting & Clearance	1.000			
2. CNI Protocol Compliance	0.574**	1.000		
3. Intelligence Sharing & Coordination	0.541**	0.568**	1.000	
4. CNI Security Effectiveness	0.684**	0.637**	0.748**	1.000

** Correlation is significant at the 0.01 level (2-tailed)

Source: Primary Data, 2026

The Pearson correlation matrix reveals a theoretically important finding: intelligence sharing and state coordination demonstrated the strongest positive correlation with CNI security effectiveness ($r = 0.748$, $p < .01$), while CNI-specific vetting despite being the most deficient governance dimension showed a smaller though significant correlation ($r = 0.684$, $p < .01$). This pattern suggested that in the CNI security context, real-time intelligence coordination between PSOs and state security agencies was the most powerful immediate effectiveness driver, reflecting the operational reality that in complex, dynamic threat environments, situational awareness and inter-agency response coordination determined security outcomes more immediately than entry-level vetting quality. However, vetting's lower mean score (2.94) combined with its significant correlation with effectiveness ($r = 0.684$) implied high marginal returns to vetting

improvement confirming that vetting enhancement, while not the strongest current predictor, represented a high-impact reform investment given the severity of the current deficit.

6.3 Regression Analysis

Table 3: Regression Model Summary-CNI Security Governance and Effectiveness

Model	R	R ²	Adj. R ²	Std. Error	F	Sig.
1	0.807	0.652	0.646	0.557	41.87	< .001

Source: Primary Data, 2026

Table 4: Regression Coefficients: Predictors of CNI Security Effectiveness, Uganda

Variable	B	SE	Beta (β)	t	Sig.
(Constant)	0.487	0.228		2.136	.034
CNI-Specific Vetting & Clearance	0.298	0.072	0.330	4.139	< .001
CNI Protocol Compliance	0.274	0.076	0.287	3.605	< .001
Intelligence Sharing & Coordination	0.384	0.074	0.372	5.189	< .001

Dependent Variable: CNI Security Effectiveness

Source: Primary Data, 2026

The regression model was significant ($F = 41.87$, $p < .001$), explaining 65.2% of variance in CNI security effectiveness ($R^2 = 0.652$). Intelligence sharing and state coordination emerged as the strongest independent predictor ($\beta = 0.372$, $p < .001$), confirming the Nodal Governance Theory's prediction that inter-nodal coordination quality was the dominant security effectiveness determinant in complex security environments. CNI-specific vetting was the second strongest predictor ($\beta = 0.330$, $p < .001$), and CNI protocol compliance contributed a significant positive effect ($\beta = 0.287$, $p < .001$).

6.4 Structural Equation Model and Path Analysis

Table 5: SEM Fit Indices: CNI Private Security Deployment Model, Uganda

Fit Index	Value	Threshold	Assessment
χ^2/df	2.09	< 3.0	Good fit
CFI	0.963	≥ 0.95	Good fit
RMSEA	0.061	< 0.08	Acceptable
SRMR	0.052	< 0.08	Good fit
GFI	0.946	≥ 0.90	Good fit

Source: Primary Data, 2026

Table 6: Structural Path Coefficients: CNI Private Security Deployment SEM, Uganda

Received: 14.09.2026

Accepted: 20.09.2026

Published on: 30.09.2026

Path	Std. β	SE	CR	p	Decision
Intelligence Sharing $\rightarrow$ CNI Security Effectiveness	0.384	0.075	5.120	< .001	Supported
CNI Vetting & Clearance $\rightarrow$ CNI Security Effectiveness	0.308	0.073	4.219	< .001	Supported
Protocol Compliance $\rightarrow$ CNI Security Effectiveness	0.261	0.077	3.390	.001	Supported
Intelligence Sharing $\rightarrow$ Protocol Compliance (med.)	0.448	0.082	5.463	< .001	Supported
Indirect: Intel.Sharing $\rightarrow$ Protocol $\rightarrow$ Effectiveness	0.137	0.043	3.186	.001	Supported
Total Effect: Intelligence Sharing $\rightarrow$ Effectiveness	0.521				
Total Effect: CNI Vetting $\rightarrow$ Effectiveness	0.308				
Total Effect: Protocol Compliance $\rightarrow$ Effectiveness	0.261				

Source: Primary Data, 2026

The structural model confirmed protocol compliance as a partial mediator of the intelligence sharing–security effectiveness relationship (indirect $\beta = 0.137$, $p = .001$), reflecting the operational logic that effective intelligence coordination informed and structured the specific security protocols deployed at CNI sites better intelligence drove better protocol specification, and better protocols generated measurably higher security effectiveness. The total effect of intelligence sharing on CNI security effectiveness ($\beta = 0.521$) substantially exceeded its direct effect ($\beta = 0.384$), confirming that intelligence integration's full security effectiveness return materialized through both the direct situational awareness channel and the protocol quality improvement channel.

7.0 Discussion, Conclusions, and Recommendations

The study confirms that CNI private security governance dimensions significantly predicted security effectiveness, with the three dimensions collectively explaining 65.2% of effectiveness variance. The dominance of intelligence sharing and state coordination (total $\beta = 0.521$) confirmed the Nodal Governance Theory's prediction that network coordination quality was the primary security effectiveness determinant in complex threat environments a finding with urgent operational implications given Uganda's impending oil production commencement and the associated threat landscape escalation. Recommendations: (i) Uganda should enact a Critical National Infrastructure Protection Act establishing a legislative framework for CNI designation, tiered security standards, and mandatory PSO-state intelligence coordination protocols; (ii) the National Information Security Agency (NISA) should establish a CNI

Received: 14.09.2026

Accepted: 20.09.2026

Published on: 30.09.2026

Security Coordination Centre providing 24-hour intelligence support to PSO site commanders at designated CNI facilities; (iii) all PSOs operating at designated CNI sites should be required to obtain a separate CNI Security Operator License with enhanced personnel vetting, specialized CNI security training, and equipment standards as prerequisites; (iv) Uganda's Ministry of Foreign Affairs should develop a Foreign Asset Security Governance Framework governing PSO deployments to diplomatic missions and foreign corporate assets, aligning Uganda's standards with Vienna Convention obligations and relevant bilateral security cooperation commitments; and (v) the Albertine Rift oil and gas Joint Operations Centre model should be formalized, replicated across all major CNI sectors, and supported by dedicated funding within the national security budget.

References

- De Witte, L. (2020). Intelligence deficits and security performance gaps in Sub-Saharan Africa oil infrastructure protection. *African Security*, 13(2), 87–112.
- International Code of Conduct Association (ICoCA). (2010). *International Code of Conduct for Private Security Service Providers*. Geneva: ICoCA.
- Isima, J. (2019). Joint operations and private security effectiveness in Nigerian oil infrastructure. *Security Dialogue*, 50(3), 248–267.
- Johnston, L., & Shearing, C. (2003). *Governing Security: Explorations in Policing and Justice*. Routledge.
- Montreux Document. (2008). *On Pertinent International Legal Obligations and Good Practices for States related to PMSC Operations in Armed Conflict*. Geneva: ICRC/Swiss FDFA.
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6), 11–25.
- Tangri, R., & Mwenda, A. (2010). President Museveni and the politics of presidential tenure in Uganda. *Journal of Eastern African Studies*, 4(2), 386–411.