TERMS OF REFERENCE
FOR
CIRT ENHANCEMENT:

February 2026

1. Background

The National Communications Authority (NCA) is the independent regulatory body for Somalia's communications sector, established under the Communications Act of 2017. Its mandate covers telecommunications, the internet, broadcasting, information and communications technology (ICT), e-commerce services, and related digital services. The NCA facilitates the development of the ICT sector, promotes fair and sustainable competition, protects consumer interests, and ensures the transparent implementation of the national communications legal framework.

Following the approval of the Cybersecurity Law in January 2026, the NCA has been formally mandated to lead the development and implementation of national cybersecurity technical infrastructure and capabilities, in collaboration with relevant government institutions. The Law places responsibility for establishing, operating, and continuously enhancing cybersecurity systems, platforms, and technical mechanisms with the NCA, with the aim of securing and protecting Somalia's cyberspace and critical digital assets.

The Somalia National Computer Incident Response Team (SOMCIRT), hosted within the NCA, serves as the national focal point for cybersecurity incident detection, response, coordination, and information sharing. SOMCIRT currently operates a foundational CERT capability, including incident intake and tracking, basic threat and vulnerability monitoring, and awareness activities. However, the increasing scale and sophistication of cyber threats necessitate targeted upgrades to technical infrastructure, analytical tools, and operational capabilities.

This assignment aims to enhance SOMCIRT and include a GovSOC function. The assignment will align with internationally recognized best practices, particularly the CSIRT Services Framework developed by FIRST. The focus is exclusively on technical, preventive, and operational CERT functions.

2. Objectives

The objective of this assignment is to enhance the operational capacity, effectiveness, and sustainability of SOMCIRT, hosted under the NCA, as the national focal point for cybersecurity incident response, coordination, and government security monitoring.

Specifically, the assignment aims to:

1. Strengthen SOMCIRT's core incident response and coordination capabilities in line with internationally recognized CSIRT best practices.
2. Improve SOMCIRT's ability to detect, analyze, manage, and respond to cybersecurity incidents affecting NCA systems and designated government and critical digital services.
3. Establish an operational Malware and Artifact Analysis capability to support incident response, threat analysis, early warning, and preventive cybersecurity.
4. Enhance proactive cybersecurity services, including alerts, advisories, threat intelligence sharing, and vulnerability coordination.
5. Establish and integrate a foundational Government Security Operations Center (GovSOC) function within SOMCIRT, providing centralized security monitoring, detection, and coordinated response for designated government systems
6. Formalize standard operating procedures (SOPs), workflows, and playbooks to ensure consistent, effective, and repeatable CERT and GovSOC operations.

7. Build institutional capacity through training, knowledge transfer, and post-implementation operational support.
8. Define operational performance indicators and internal service targets for the enhanced CIRT and GovSOC capabilities.
9. Strengthen national cybersecurity governance, escalation, and information sharing arrangements between SOMCIRT, government entities, and critical information infrastructure operators.
10. Ensure sustainability through a structured operational transition plan and a multi year SOMCIRT and GovSOC maturity roadmap.

The assignment shall **not** include digital forensics, evidence handling, chain-of-custody processes, law-enforcement support, or judicial/prosecutorial functions.

3. Scope of Work

The scope of this assignment is limited to enhancing the Somalia National Computer Incident Response Team (SOMCIRT) and establishing an operational Malware and Artifact Analysis capability, while also standing up a foundational Government Security Operations Center (GovSOC) function within SOMCIRT to support centralized security monitoring and coordinate incident triage for designated government systems. The scope focuses exclusively on technical, operational, and preventive cybersecurity functions, including CERT coordination, incident handling, malware and artifact analysis, threat intelligence, and foundational government security monitoring, consistent with the CSIRT Services Framework developed by FIRST and recognized good practice for hybrid CERT–GovSOC models. The GovSOC capability established under this assignment shall be foundational, focusing on visibility, alerting, and coordination, and shall not constitute a fully staffed, fully automated, or 24/7 security operations center, which will be addressed in subsequent phases. The assignment excludes law enforcement, investigative, digital forensic, evidentiary, and prosecutorial activities. Implementation shall follow a design-and-build approach, with the Consultant proposing detailed architectures, configurations, and quantities aligned with the requirements outlined below.

3.1 CIRT Operational Enhancement

The Consultant shall enhance SOMCIRT's core CERT operations to enable effective detection, analysis, response, and coordination of cybersecurity incidents affecting NCA systems and connected government and critical digital services.

This shall include:

- A technical review of the current SOMCIRT environment, including infrastructure, tools, workflows, and service maturity.
- Strengthening end-to-end incident handling processes, covering incident intake, validation, triage, prioritization, technical analysis, coordination, escalation, closure, and post-incident review.
- Development and implementation of standardized incident response workflows and playbooks for common incident categories (e.g., malware, phishing, denial-of-service).
- Establishment of secure communication and coordination mechanisms for trusted information exchange with designated government and sectoral focal points.

- Definition and documentation of operational governance arrangements, including roles and responsibilities, a RACI matrix, escalation paths, decision and approval boundaries, and information-sharing procedures among SOMCIRT, NCA, designated government entities, and participating critical information infrastructure operators.
- Integration of security monitoring inputs into CERT operations to support centralized triage and coordinated response in coordination with the GovSOC function established under this assignment.

3.2 GovSOC Technical Coverage and Capacity

The enhancement shall include the following defined coverage and capacity parameters, which shall guide the design-and-build proposals. The quantities below are indicative baseline assumptions and may be refined by the Consultant as part of the proposed technical architecture, subject to NCA approval.

- **Endpoint Detection and Response (EDR/XDR)**
  Deployment of an EDR/XDR capability for designated government systems, integrated with SOMCIRT to enable centralized endpoint detection and coordinated incident response.

Coverage: four (4) servers.

- **Server Security Monitoring:**
  Integration of security monitoring for government and digital services to enable centralized incident triage and coordinated response across government systems and critical information infrastructure.
  Coverage: Four (4) servers.
- **Processing and Storage Capacity:**
  Establishment of a centralized log and event analytics capability to support threat analysis, correlation, investigation support, and government level reporting. *Capacity:* Two (2) servers dedicated to processing and storage.

  - **Centralized Architecture:**

    Implementation of a centralized national CSIRT platform operated by SOMCIRT and connected to government and sectoral focal points through secure channels. *Platform:* One (1) centralized CSIRT platform.

  - **Deployment Model:**
    Adoption of a **hybrid deployment model**, with:

    - Core operational platforms hosted on premises within a secure SOMCIRT facility; and
    - Elastic analytics, backup, and resilience services hosted in trusted cloud environments. *Configuration:* One (1) on-premises environment and one (1) cloud environment.
    - The design shall include secure backup and restoration arrangements, configuration and data recovery procedures, recovery priorities, proportionate platform availability requirements, and periodic recovery testing. The Consultant shall identify options and prerequisites for future disaster recovery capability; implementation of a separate secondary disaster recovery site or a full enterprise business continuity management

system is outside the scope of this foundational phase unless specifically approved by NCA.

3.3 Establishment of a Malware and Artifact Analysis Capability

The Consultant shall design, deploy, and operationalize a secure, scalable, and isolated Malware and Artifact Analysis Capability to support SOMCIRT's incident response, threat analysis, and national early-warning functions. The capability shall be strictly defensive and analytical, and shall not include digital forensics, evidentiary, or law enforcement functions.

3.3.1 Malware Analysis Environment Architecture and Design

The Consultant shall design the logical and physical architecture of the Malware Analysis Environment to ensure high levels of isolation, safety, and operational resilience. The design shall include:

- Secure logical and physical architecture of the Malware Analysis Environment.
- Network segmentation and isolation mechanisms, including air-gapped or tightly controlled connectivity.
- Clear separation between analysis, management, and reporting environments.
- Secure access control, authentication, logging, and monitoring mechanisms.
- Alignment and controlled integration with SOMCIRT's existing SOC functions, incident management systems, and threat-intelligence platforms.

The architecture shall ensure safe handling of malicious artifacts and prevent accidental propagation, leakage, or compromise of production or operational networks.

3.3.2 Malware Analysis Capabilities

The Malware Analysis Environment shall support operational malware analysis, including but not limited to the following:

a) Static Analysis

- File type identification and metadata extraction.
- Cryptographic hashing and signature generation.
- String analysis and obfuscation detection.
- Code structure inspection and packer identification.

b) Dynamic and Behavioral Analysis

- Execution of malware in controlled and instrumented sandbox environments.
- Monitoring of file system, registry, process, and network behavior.
- Detection and analysis of command-and-control (C2) communications.
- Analysis of persistence, privilege escalation, and lateral movement techniques.

c) Artifact and Indicator Extraction

- Extraction and validation of indicators of compromise (IOCs), including hashes, IP addresses, domains, URLs, and mutexes.

- Mapping of observed malware behavior to recognized attack techniques (e.g., MITRE ATT&CK).
- Correlation of malware artifacts with ongoing incidents, alerts, and campaigns.

All analysis activities shall be conducted solely to support incident response, threat mitigation, and preventive CERT operations.

3.3.3 Tooling and Technology Stack

The Consultant shall propose, deploy, and configure an appropriate tooling stack for malware and artifact analysis, prioritizing open-source, interoperable, and widely adopted solutions. The stack may include:

- Malware sandboxing and detonation platforms.
- Reverse-engineering and disassembly tools.
- Memory and network traffic analysis tools.
- Artifact parsing and indicator extraction tools.
- Secure repositories for malware samples, analysis outputs, and reports.

All tools shall:

- Be legally permissible and ethically appropriate for CERT operations.
- Integrate with SOMCIRT's existing platforms, including SIEM, SOAR, threat-intelligence platforms, and case management systems used to support GovSOC and CERT functions.
- Support automation, enrichment, and playbook-driven workflows.

3.3.4 Integration with SOMCIRT Operations

The Malware Analysis Environment shall be fully integrated into SOMCIRT's operational environment and workflows, including:

- Incident intake, triage, and investigation processes.
- Threat-intelligence ingestion, enrichment, and dissemination.
- SOC alert validation, correlation, and escalation.
- National early-warning, alerting, and advisory issuance.
- Secure information sharing with trusted government and critical-sector stakeholders.

Standard Operating Procedures (SOPs) shall be developed to ensure consistent, repeatable, and auditable use of the Malware Analysis capability in SOMCIRT operations.

3.3.5 Policies, Procedures, and Governance

The Consultant shall develop and document policies and procedures governing the safe and responsible operation of the Malware Analysis Environment, including:

- Malware handling and safety procedures.
- Sample intake, storage, retention, and disposal policies.
- Access control and authorization procedures.
- Risk management and acceptable-use policies for the Environment .
- Ethical and legal compliance guidelines applicable to CERT operations.

These documents shall form part of SOMCIRT's internal governance and operational framework.

3.4 Integration Scope

The enhanced CIRT platform shall be integrated into a unified operational environment, including integration with:

- Existing vulnerability scanning tools
- Threat intelligence platforms and feeds
- Secure information-sharing channels
- Firewall and Web Application Firewall (WAF) logs
- Honeypot sensors
- The national incident reporting portal
- Secure email and alerting systems

All integrations shall support centralized visibility, analysis, and coordinated incident response. Operational response actions on monitored systems shall remain under the authority of the respective system owning entities.

3.5 Operational Capacity Building and Cyber Drill Program

To ensure operational readiness and effective use of the enhanced CIRT, Malware Analysis, and foundational GovSOC capabilities, the Consultant shall implement a structured operational capacity-building program for SOMCIRT personnel.

The program shall include:

1. **Operational Skills Assessment**
   A focused assessment to identify priority skill gaps in incident detection, triage, response coordination, malware analysis, threat intelligence integration, and GovSOC monitoring workflows.
2. **Hands-On Technical Training**
   Delivery of practice-oriented technical training aligned with the deployed platforms (SIEM, SOAR, EDR/XDR, Malware Analysis Environment), emphasizing real-world incident handling, coordinated response procedures, and use of operational playbooks.
3. **Cyber Drills and Simulations**
   Design and execution of structured cyber drills simulating realistic cyber incident scenarios (e.g., malware outbreaks, phishing campaigns, coordinated attacks), covering detection, analysis, containment, communication, and post-incident review.

All capacity-building activities shall be directly aligned with the enhanced CIRT and GovSOC architecture deployed under this assignment.

3.6 Institutionalization and Post-Go-Live Operations

To ensure sustainability, the Consultant shall:

- Develop and document standard operating procedures (SOPs) and operational guidelines for all enhanced CERT services.

- Provide hands-on training and knowledge transfer to SOMCIRT technical staff.
- Conduct operational simulations and tabletop exercises.
- Define a practical performance measurement framework with baseline key performance indicators (KPIs) and internal service targets for incident acknowledgement, triage, escalation, response coordination, monitoring coverage, platform availability, playbook use, and operational readiness. The targets shall reflect the foundational, non-24/7 GovSOC model and dependencies on participating system owners.
- Develop a structured operational transition and sustainability plan covering handover milestones, knowledge-transfer responsibilities, competency targets, recommended staffing profiles, recurring licensing and maintenance needs.
- Conduct a handover readiness assessment prior to final acceptance and submit an exit report at the end of the post go live support period, confirming SOMCIRT's operational readiness and any residual gaps.
- Prepare a three-year SOMCIRT and GovSOC maturity roadmap identifying sequenced capability improvements, dependencies, and prerequisites for future expansion, including possible 24/7 operations.
- Support SOMCIRT during a twelve (12) month post-go-live support period, after which SOMCIRT shall operate, maintain, and continuously improve the platform as the national focal point for cybersecurity incident response and coordination and government security monitoring.

4 Deliverables

The Consultant shall deliver the following outputs in accordance with the approved work plan and implementation schedule.

4.1 CIRT Enhancement Deliverables

The Consultant shall provide:

- Fully installed, configured, and operational CIRT and GovSOC hardware and software components in accordance with the approved design.
- Configured and integrated security monitoring and response platforms, supporting the GovSOC function within SOMCIRT, including:
    - Security Information and Event Management (SIEM)
    - Security Orchestration, Automation and Response (SOAR)
    - Threat Intelligence Platform (TIP)
    - Endpoint and server detection and monitoring systems are deployed for designated government systems
- Operational incident response tools and secure communication systems that support CERT coordination, GovSOC alert handling, and information sharing.
- Enhanced CIRT and GovSOC logical and physical architecture diagrams, network designs, and system configuration documentation.

- Operational Malware and Artifact Analysis environment fully deployed, tested, and integrated with SOMCIRT platforms.
- Functional testing and validation of all deployed systems and integrations, including documented test cases and acceptance results.

4.2 Malware Analysis Capability Deliverables

The Consultant shall deliver:

- Fully operational Malware and Artifact Analysis Environment, including:
    - Secure and isolated analysis environments
    - Sandboxing and malware detonation platforms
    - Static and dynamic malware analysis toolchains
- Integrated workflows linking malware analysis outputs to incident management, threat intelligence platforms, GovSOC alert handling, and response playbooks.
- Documented malware analysis procedures, safety controls, and operational workflows, aligned with CERT defensive and preventive functions.
- Demonstrated capability to extract, correlate, and disseminate indicators of compromise (IOCs) to support CERT operations, national early-warning, and advisory issuance.

4.3 Capacity Building and Operational Readiness Deliverables

The Consultant shall deliver the following measurable outputs:

1. **Operational Skills Assessment Report**
    - One (1) focused training needs assessment identifying operational skill gaps and mapping priority training areas.
2. **Hands-On Technical Training Sessions**
    - Minimum **one (1) instructor-led technical training session**, aligned with deployed CIRT and GovSOC tools and workflows.
    - Each session shall include practical exercises and lab-based components.
    - Training attendance sheets and materials shall be submitted.
3. **Cyber Drills and Simulations**
    - Minimum **two (2) structured cyber drills**, including:
        - At least **one (1) tabletop exercise**
        - **At least one (1) technical simulation exercise**
    - Delivery of After-Action Reports for each drill, documenting performance, identifying gaps, and recommending improvements.
4. **Final Capacity Building Report**
    - Consolidated report including:
        - Summary of training delivered
        - Drill performance evaluation results
        - Identified operational gaps
        - Recommendations for continuous operational improvement

4.4 Documentation Deliverables

The Consultant shall provide complete and up-to-date documentation, including:

- System configuration and architecture documentation.
- User manuals and operational guides for all deployed platforms.
- Standard Operating Procedures (SOPs) for incident response, malware analysis, and threat intelligence workflows.
- Maintenance, troubleshooting, and escalation guides.
- Licensing, warranty, and support documentation for all hardware and software components.
- Final system handover and acceptance documentation.
- Operational governance and coordination framework, including the RACI matrix, escalation procedures, approval boundaries, and information-sharing protocols.
- Operational KPI and internal service-target framework, including definitions, data sources, baseline values, reporting frequency, and review arrangements.
- Backup, restoration, service-continuity, and recovery procedures, together with recovery-test results and recommendations for future disaster recovery capability.
- Operational transition and sustainability plan, including competency targets, recommended staffing profiles, recurring support requirements, and indicative operating-cost categories.
- Three-year SOMCIRT and GovSOC maturity roadmap.
- **Handover readiness assessment and end-of-support exit report.**

All documentation shall be delivered in both editable format and final PDF format.

Duration and Payment Milestones

5.1 Duration

The assignment shall be implemented in two clearly defined phases:

1. **Implementation Phase** – covering inception, detailed design, system deployment, integration, operationalization, training, documentation, testing, and formal handover. This phase shall be completed within approximately **six (6) months** of the contract start date.

2. **Post-Go-Live Support**– covering operational support, fine-tuning, troubleshooting, and knowledge reinforcement for the deployed CIRT, Malware Analysis, and foundational GovSOC capabilities.
   This phase shall extend for **twelve (12) months** after formal system handover and acceptance.

The total assignment duration shall therefore be approximately **eighteen (18) months**, inclusive of post-go-live support.

5.2 Payment Milestones

Payments to the Consultant shall be made upon satisfactory completion and formal acceptance of milestone deliverables by the National Communications Authority (NCA), in accordance with the milestone-based schedule below.

Milestone	Key Deliverables	Indicative Timeline (Weeks)	Payment (%)
Milestone 1 – Inception and Detailed Design	• Inception Report and detailed work plan • Technical assessment of existing SOMCIRT environment • Target architecture and detailed design for CIRT enhancement, Malware & Artifact Analysis Environment, and foundational GovSOC • Initial operational governance model, KPI framework, continuity requirements, sustainability approach, and maturity-roadmap methodology	Weeks 1–2	20%
Milestone 2 – System Deployment and Integration	• Installation and configuration of CIRT and foundational GovSOC platforms • Deployment of security monitoring, incident management, automation, and endpoint/server monitoring capabilities • Deployment and integration of the Malware & Artifact Analysis Environment • Initial system integrations and configuration testing	Weeks 3–12	30%
Milestone 3 – Operationalization	• Fully operational Enhanced CIRT, Malware Analysis, and foundational GovSOC workflows • Integrated incident response, malware analysis, and threat intelligence processes • Operational simulations and functional validation exercises	Weeks 13–20	30%
Milestone 4 – Final Acceptance and Handover	• Final system testing and acceptance • Delivery of all SOPs, operational manuals, and documentation • Formal system go-live and handover to SOMCIRT • Final Completion and Acceptance Report Final operational governance, KPI, resilience, transition and sustainability, and three-year maturity-roadmap package	Weeks 21–26	20%

5.3 Post-Go-Live Support

Following completion of Milestone 4, the Consultant shall provide twelve (12) months of post-go-live support, including:

- Operational support and troubleshooting;
- Fine-tuning of configurations and workflows;
- Support during live incident handling, as required.

- Knowledge reinforcement and limited refresher support.
- Monitoring and reporting against the agreed operational KPIs and internal service targets;
- At least one documented backup-restoration and service-recovery test;
- Progressive transfer of administrative and operational responsibilities to SOMCIRT in accordance with the approved transition plan.

The Consultants are invited to suggest alternative timelines in their proposals.

6. Reporting and Governance

- The Consultant shall report to the designated NCA/SOMCIRT Engagement Manager.
- The Consultant shall submit monthly progress reports, or at another frequency agreed during inception, covering implementation progress, risks, dependencies, decisions required, and planned activities.
- Deliverables affecting connected government systems shall be reviewed with the relevant system-owning entity through NCA-coordinated validation arrangements.
- Inception report (within two weeks of contract start)
- Midterm progress report
- Final Completion and handover package.

7. Support, Warranty, and Maintenance

The consultant shall provide:

- Hardware warranty of at least 1–3 years.
- Software licensing (annual renewal plans)
- 24/7 technical support and remote assistance (duration 1 year)
- Periodic maintenance visits
- Updates and patches for all software

8. Ethical and Legal Compliance

All activities shall comply with:

- National cybersecurity laws of Somalia
- Data protection and privacy principles
- International standards and best practices:
    - **ISO/IEC 27035 (Incident Management)**
    - NIST Cybersecurity Framework
    - Malabo Convention on Cyber Security

9. Client Responsibilities

- The deliverables procured through this engagement are advisory in nature. The National Communications Authority (NCA) will appoint a qualified person to serve as Engagement Manager to oversee the engagement.
- The National Communications Authority (NCA) will provide the consultant with relevant documents, including policies, strategies, risk assessments, and other information to support

the consultant in delivering the expected outcomes. The National Communications Authority (NCA) will make subject-matter experts available for interviews and information-gathering.

- The National Communications Authority (NCA) will assist with identifying stakeholders and preparing interview documentation in a timely manner.
- The National Communications Authority (NCA) will be responsible for all management decisions relating to the engagement and resulting deliverables, the use or implementation of the engagement, the output, and for the determination of whether the deliverables are appropriate for their purposes.
- The National Communications Authority (NCA) will own the intellectual property rights of the deliverables created through this engagement.

10. Required Experience: Firm and Core Team

The firm selected will need to demonstrate:

- Having strong skills and experience in cybersecurity and Information and Communication Technologies (ICT), particularly in the following areas: incident response, cyber threat intelligence, with at least 5 years of relevant experience.
- At least 3 project references in the past 5 years of Integrating and customization of CSIRT/CERT/CIRT/SOC Tools; Developing policies and procedures related to CSIRT/CERT/CIRT/SOC operations (operational workflows, SOPs, incident management processes, service level management frameworks, among others);
- Setting up cybersecurity operations center tools, configuring honeypots, integrating external threat-intelligence feeds, and implementing related incident-detection and response capabilities.
- Extensive knowledge of cybersecurity policy, strategy, and operations in a government context.
- Demonstrating an understanding of relevant frameworks, methodologies, and best practices in cybersecurity and incident response.
- Prior experience working with the public sector is preferred.
- Experience in a developing country context is considered an advantage.

The firm shall propose a core team, at a minimum, comprising (1) Team Leader, (1) Incident Response specialist, (1) Cybersecurity Governance and Risk Management specialist, (1) Malware Analyst, (1) SOC Analyst, plus any additional support staff deemed necessary to deliver the assignment

Key Position Experience Qualifications:

1. Team Leader, or equivalent

The Team Leader must hold master's degree in Cybersecurity, Information Security, Computer Science, Telecommunications or other relevant fields. The team leader must demonstrate a minimum seven (7) years of cybersecurity programme or project management experience, specifically in incident response, cyber threat intelligence, and CSIRT/SOC implementation.

The team leader must have Proven experience in managing and implementing CIRT/CERT/CSIRT/SOC-related projects in developing countries or post conflict countries. The Team leader must hold recognized project management certification and should have at least one of the following certifications, CISSP, CISM, or GCIH.

2. **Incident Response Specialist:**

The Incident Response Specialist must hold master's degree in Cybersecurity, Information Security, Computer Science, Telecommunications or other relevant fields. The Specialist must demonstrate at least five (5) years of experience in cybersecurity incident response, with a focus on establishing and managing CIRTs. In-depth knowledge of incident response and CIRT establishment frameworks and methodologies, such as the FIRST CSIRT Services Framework, NIST SP 800-61, ISO/IEC 27035, and the SANS Incident Handling methodology, and their application to building and operating effective CIRTs. The Specialist should hold at least one recognized certification, such as Certified Information Systems Security Professional (CISSP), GIAC Certified Incident Handler (GCIH), or EC-Council Certified Incident Handler (ECIH).

Also, the specialist must have proven ability to design and implement incident response policies, procedures, and workflows, and to train and mentor CIRT members on incident response best practices.

3. **Governance and Risk Management Specialist**

The Governance and Risk Management Specialist must hold a master's degree in Cybersecurity, Information Security, Telecommunications, Computer Science, or other relevant fields. The Specialist must demonstrate a minimum five (5) years of relevant professional experience in cybersecurity governance, risk management, compliance, and critical information infrastructure protection (CIIP), preferably at the national or public-sector level. In-depth knowledge of recognized cybersecurity risk management and CIIP frameworks, including NIST SP 800-53, ISO/IEC 27001, and CIP-014-1, and their application to the protection of critical information infrastructure. The Specialist should hold at least one recognized certification, such as Certified Information Systems Security Professional (CISSP), ISO/IEC 27001, Certified Information Security Manager (CISM), or Certified Critical Infrastructure Protection Professional (CCIPP).

4. **Malware Analyst**

The Malware Analyst must hold a master's degree in Cybersecurity, Computer Science, Information Security, Telecommunications, or a related field, with at least five (5) years of experience in malware analysis, cyber threat intelligence, or incident response, preferably at the national or critical information infrastructure level. The Analyst should have experience in static and dynamic malware analysis, reverse engineering, threat hunting, and incident investigation, with hands-on experience using debuggers, disassemblers, and tools such as IDA Pro and Ghidra, as well as SIEM and EDR platforms. Proficiency in scripting and programming (e.g., Python, C, JavaScript, VBScript), strong knowledge of operating systems, processor architectures, and computer networking, and the ability to clearly communicate complex technical findings are essential. The Analyst should hold at least one recognized certification, such as GREM, GCFA, GCIH, CEH, or CISSP.

5. **SOC Analyst**

The SOC Analyst must hold a master's degree in Cybersecurity, Information Security, Computer Science, Telecommunication or a related discipline, with a minimum of five (5) years of demonstrable experience in Security Operations, Threat Detection, and Incident Response within enterprise or critical infrastructure environments. The Analyst must demonstrate advanced proficiency in SIEM platforms (Splunk, IBM QRadar, Microsoft Sentinel), EDR/XDR solutions, IDS/IPS, firewall, and network traffic analysis, log correlation, and threat intelligence integration using frameworks such as MITRE ATT&CK. The Analyst must have proven hands-on expertise in malware triage, vulnerability assessment, packet analysis, and security automation using

Python, PowerShell, or Bash. The Analyst's experience must align with recognized standards and frameworks, including NIST SP 800-61, the NIST Cybersecurity Framework (CSF), and ISO/IEC 27001 incident management processes. The Analyst must hold at least one recognized professional certification, such as CompTIA CySA+, CEH, GCDA, GCFA, OSCP, GCIH, GCIA, or CISSP.

11. Contracting and Reporting Arrangements

The NCA will contract the consultancy firm, which will be required to work closely with a designated focal point. The firm is expected to submit all deliverables electronically in PDF and editable Word formats. The consultant may also be required to present deliverables in person or virtually for validation. The NCA focal point will monitor the assignment's progress to ensure alignment with project objectives.

12. Timeframe

The assignment is expected to be completed within **eighteen (18)** months from the start date.