HIGH INTENSITY DRUG TRAFFICKING AREAS (HIDTA)
NATIONAL HIDTA ASSISTANCE CENTER (NHAC)

Contract Opportunity
Location: National HIDTA Assistance Center – Miami, Florida (Remote Work Allowed, Preference Given to a Candidate Living Near a HIDTA Headquarters Facility, HIDTA map)
Position: National HIDTA Information Security and Technology Director
Compensation: Commensurate with the Federal Senior Executive Service Pay Scale
Closing Date: Letter of Interest and Resume Must Be Received by 05/01/26

The position of National HIDTA Information Security and Technology Director is a senior position within the National HIDTA Assistance Center (NHAC) reporting to the Director o f the NHAC and coordinating closely with the HIDTA Director and Chairman of the HIDTA Information Technology Committee, the HIDTA Information Technology Advisory Council, and the Office of National Drug Control Policy (ONDCP). This position is responsible for assessing the IT posture and cybersecurity of the various HIDTA programs in the United States; assisting in the formulation of Information Security and Technology policies for the National HIDTA Program; providing guidance, advice, and assistance to the 33 HIDTA Directors in the United States on Information Security and Technology matters including third party assessment of the HIDTAs; assisting the 33 HIDTA programs in the selection and evaluation (as necessary) of Information Technology personnel or potential hires; assisting the various regional HIDTA programs in all aspects of information technology and security design and implementation, and in assisting the Office of National Drug Control Policy (ONDCP) in establishing national HIDTA Information Technology and Guidance. This position will be directed by the National HIDTA Assistance Center (NHAC) in Miami, Florida, but the selected candidate may live in any location in the continental United States, with preference given to a qualified applicant who lives near a HIDTA location.

Responsibilities:

Strategic Leadership & Policy

- Serve as the principal cybersecurity advisor to NHAC, HIDTA leadership, and ONDCP.
- Develop and implement enterprise-wide cybersecurity strategies, policies, and governance frameworks.
- Lead integration of cybersecurity with law enforcement and IT mission operations.
- Represent HIDTA in federal, interagency, and national cybersecurity policy initiatives.
- Formulate long-range cybersecurity policies and drive adoption across distributed environments.

Cybersecurity Program Management & Compliance

- Lead development and execution of cybersecurity programs, including training, audits, and compliance.
- Ensure adherence to federal mandates and reporting requirements, including FISMA and OMB directives.
- Oversee cybersecurity audits, reporting, and remediation of findings.
- Establish cybersecurity awareness programs, dashboards, and performance metrics.

- Coordinate responses to oversight bodies (e.g., GAO, OMB, and other federal entities).

Risk Management, Assessments & Supply Chain Security

- Conduct and oversee enterprise-wide risk, threat, and vulnerability assessments.
- Provide actionable recommendations to HIDTA Directors and governing bodies.
- Lead Cyber Supply Chain Risk Management (C-SCRM) efforts across the HIDTA ecosystem.
- Evaluate IT systems, vendors, and managed service providers for risk and performance.
- Support disaster recovery planning and Privacy Impact Assessments.

Security Operations & Incident Response

- Provide executive oversight of cybersecurity operations, including SOC capabilities and monitoring.
- Lead incident detection, response, and recovery efforts across HIDTA environments.
- Coordinate with federal, state, and local partners, including law enforcement and DHS.
- Advise leadership on active threats, system compromises, and mitigation strategies.
- Ensure alignment with national frameworks and continuous improvement of response capabilities.

Insider Threat & Advanced Security Programs

- Develop and oversee insider threat detection and prevention programs.
- Implement user activity monitoring, behavioral analytics, and SIEM capabilities.
- Coordinate with legal, HR, and leadership to enforce security policies.
- Continuously assess and enhance insider threat mitigation strategies.

Technology Evaluation & Enterprise Integration

- Evaluate emerging cybersecurity technologies and IT systems.
- Provide guidance on IT procurement, architecture, and modernization initiatives.
- Integrate cybersecurity into enterprise architecture and system design.
- Address infrastructure, performance, and capacity challenges.

Workforce Development & Advisory Services

- Identify training gaps and lead cybersecurity workforce development initiatives.
- Support hiring, evaluation, and development of IT and cybersecurity personnel.
- Serve as a senior subject matter expert and trusted advisor across HIDTA regions.
- Foster collaboration and build high-performing, mission-focused teams.

Stakeholder Engagement & Communication

- Coordinate with ONDCP on policy, budget guidance, and national strategy.
- Liaise with federal, state, and local partners on cybersecurity initiatives.
- Deliver executive briefings, reports, and strategic recommendations.
- Build consensus across diverse stakeholders and technical environments.

EDUCATION/EXPERIENCE:

- 10+ years of progressive hands-on experience in the management of Cybersecurity and Incident Response and other Information Technology functions on behalf of a Federal, state, or local law enforcement agency, or a government entity with oversight of law enforcement information technology security and needs.
- Experience in developing and implementing cybersecurity and information technology policies and programs.
- Experience in cybersecurity frameworks such as NIST, ISO 27001/2, CJIS, and other applicable security standards.
- Experience with developing and implementing Cybersecurity Resilience programs, Incident Response efforts, and cybersecurity training to assist in effectively securing HIDTA critical data.
- Experience in the development and implementation of Privacy Impact Assessment.
- Experience in Network Security, Firewall and System Access programs, and Penetration Testing to ensure network security and stability.
- Prior experience in conducting system information security audits, preparing cybersecurity audit reports, and developing responses to audit findings.
- Possess strong critical thinking and communication skills to effectively communicate critical cybersecurity and information technology to various stakeholders, bot verbally, and in writing.
- Ability to prepare documentation, policies and build consensus across a broad group.
- Bachelor's degree or higher in Computer Science or related discipline.

OTHER REQUIREMENTS:

- Be a US Citizen and ability to pass a law enforcement background and obtain a Federal security clearance at the Top Secret level.
- Ability to communicate effectively in writing and orally, including relaying complex or specialized information to a lay audience in English. Strong writing skills in English.
- Ability to interact well with others.
- Ability to communicate effectively in writing and orally, including relaying complex or specialized information to a lay audience.
- Strong analytical skills.
- Strong writing skills.
- Ability to employ sound research methods.
- Ability to organize and prioritize work.
- Ability to work with little or no supervision.
- Ability to handle multi-tasking.
- Knowledge of the executive/legislative decision-making process.
- Meet deadlines in a timely manner.
- Skill in transmitting information by spoken word to audiences with differing levels of comprehension.
- Skill in presenting concepts orally in achieving understanding of a point of view in a structured setting.

TRAVEL REQUIREMENTS

This position will require significant travel to individual HIDTAs and to HIDTA meetings at the national level.

SUPERVISORY CONTROLS:
This position has no supervisory authority.

PHYSICAL DEMANDS:
This position requires extensive time sitting at a computer workstation.

WORK ENVIRONMENT:
The work requires no risks or discomforts and is typically performed in an office setting.

COMPENSATION:
This is an annually renewed contract position based on available funding and need. The Contractor will invoice for their services monthly.

There is no relocation funding available for this position.

APPLICATION AND PROCEDURE DEADLINE:
Individuals with the requisite skills interested in providing contract services to the NHAC are invited to submit a packet responding to this announcement. The packet shall consist of a letter of interest that states the individual's willingness to contract with the NHAC and that summarizes the individual's qualifications to provide the services described in this announcement. A resume supporting the stated qualifications shall be included as an attachment to the letter of interest. Packets should be e-mailed to: Maria Zamora mfzamora@nhac.org no later than 5/1/26. Any submissions received after this date will not be considered.