JOSH B. GREEN, M.D.
GOVERNOR
KE KIA'ĀINA

BONNIE KAHAKUI
ADMINISTRATOR

DAYNA OMIYA
ASSISTANT ADMINISTRATOR

STATE OF HAWAIʻI | KA MOKUʻĀINA O HAWAIʻI

STATE PROCUREMENT OFFICE

P.O. Box 119
Honolulu, Hawaii 96810-0119
Tel: (808) 586-0554
email: state.procurement.office@hawaii.gov
http://spo.hawaii.gov

March 24, 2026

TO:

Executive Departments/Agencies
Department of Education
School Facilities Authority
Hawaii Health Systems Corporation
Office of Hawaiian Affairs
University of Hawaii
Public Charter School Commission and Schools
House of Representatives
Senate
Judiciary

City and County of Honolulu
Honolulu City Council
Honolulu Board of Water Supply
Honolulu Authority for Rapid Transportation
County of Hawaii
Hawaii County Council
County of Hawaii-Department of Water Supply
County of Maui
Maui County Council
County of Maui-Department of Water Supply
County of Kauai
Kauai County Council
County of Kauai – Department of Water

FROM: Bonnie Kahakui, Administrator

SUBJECT: **Change No. 1**
SPO Price List Contract No. 26-09
NASPO VALUEPOINT CYBERSECURITY AND INFORMATION SECURITY SERVICES
RFP No. 928
Expires: October 31, 2026

The following changes were made to the price list contract:

1. 22nd Century Technologies Inc. and Global Solutions Group Inc were added to the price list contract.
2. The point of contact for the University of Hawaii was updated.

The current price list contract incorporating Change No. 1 is available on the SPO website: http://spo.hawaii.gov. Click on *Price & Vendor List Contracts* on the home page.

If you have any questions, please contact Matthew Chow at (808) 586-0577 or matthew.m.chow@hawaii.gov.

TABLE OF CONTENTS

STATE OF HAWAII

STATE PROCUREMENT OFFICE

SPO Price List Contract No. 26-09
Includes Change No. 1
Effective: 03/24/2026

THIS SPO PRICE/VENDOR LIST CONTRACT IS FOR AUTHORIZED BUSINESS ONLY

NASPO VALUEPOINT
CYBERSECURITY AND INFORMATION SECURITY SERVICES
(RFP No. 928)
February 23, 2026 to October 31, 2026

INFORMATION ON NASPO VALUEPOINT

The NASPO ValuePoint Cooperative Purchasing Organization is a multi-state contracting consortium of state governments, including local governments, of which the State of Hawaii is a member. NASPO ValuePoint Purchasing Organization seeks to achieve price discounts by combining the requirements of multi-state governmental agencies, and cost-effective and efficient acquisition of quality products and services.

The State of Idaho is the current lead agency and contract administrator for the NASPO ValuePoint Cybersecurity and Information Security Services contract. A request for competitive sealed proposals was issued on behalf of NASPO ValuePoint Cooperative Purchasing Organization and contracts were awarded to eleven (11) qualified Contractors.

The contract provides Category 1 – Risk Assessment and Mitigation Services, Category 2 – Incident Response Services, Category 3 – Breach Coach Services and Category 4 – Notification and Credit Monitoring Services.

For additional information on this contract, visit the NASPO ValuePoint website at https://www.naspovaluepoint.org/portfolio/cybersecurity-information-security-services-2025-2031/.

PARTICIPATING JURISDICTIONS listed below have signed a cooperative agreement with the SPO and are authorized to utilize this price list contract.

Executive Departments/Agencies

Department of Education (DOE)
School Facilities Authority (SFA)

Hawaii Health Systems Corporation (HHSC)

Office of Hawaiian Affairs (OHA)
University of Hawaii (UH)

Public Charter School Commission and Schools

House of Representatives (House)
Senate

Judiciary

City and County of Honolulu (C&C Honolulu)
Honolulu City Council
Honolulu Board of Water Supply
Honolulu Authority for Rapid Transportation (HART)
County of Hawaii
Hawaii County Council
County of Hawaii – Department of Water Supply
County of Maui
Maui County Council
County of Maui – Department of Water Supply
County of Kauai
Kauai County Council
County of Kauai – Department of Water

The participating jurisdictions are not required but may purchase from this price list contract, and requests for exception from the contract are not required. Participating jurisdictions are allowed to purchase from other contractors; however, HRS chapter 103D, and the procurement rules apply to purchases by using the applicable method of procurement and its procedures, such as small purchases or competitive sealed bidding. The decision to use this contract or to solicit pricing from other sources is at the discretion of the participating jurisdiction.

POINTS OF CONTACT. Questions regarding the products listed, ordering, pricing and status should be directed to the contractor(s).

Procurement questions or concerns may be directed as follows:

Jurisdiction	Name	Telephone	FAX	E-mail
Executive	Matthew Chow	586-0577	586-0570	matthew.m.chow@hawaii.gov
DOE	Procurement Staff	675-0130	675-0133	G-OFS-DOE-Procurement@k12.hi.us
SFA	Gaudencia "Cindy" Watarida	430-5531	n/a	cindy.watarida@k12.hi.us
HHSC	Nancy Delima	359-0994	n/a	ndelima@hhsc.org
OHA	Christopher Stanley	594-1833	594-1865	psp@oha.org
OHA	Gary Garo	582-0526	594-1865	travelservices@oha.org
UH	Bonnie Anderson	956-8687	956-2093	bonnie27@hawaii.edu

Jurisdiction	Name	Telephone	FAX	E-mail
Public Charter School Commission and Schools	Danny Vasconcellos	586-3775	586-3776	danny.vasconcellos@spcsc.hawaii.gov
House	Brian Takeshita	586-6423	586-6401	takeshita@capitol.hawaii.gov
Senate	Carol Taniguchi	586-6720	586-6719	c.taniguchi@capitol.hawaii.gov
Judiciary	Tritia Cruz	538-5805	538-5802	tritia.l.cruz@courts.hawaii.gov
Honolulu City and County (C&C)	Procurement Specialist	768-5535	768-3299	bfspurchasing@honolulu.gov
Honolulu City Council	Kendall Amazaki, Jr.	768-5084	n/a	kamazaki@honolulu.gov
Honolulu City Council	Nanette Saito	768-5085	768-5011	nsaito@honolulu.gov
Honolulu Board of Water Supply	Procurement Office	748-5071	n/a	fn_procurement@hbws.org
HART	Dean Matro	768-6246	n/a	dean.matro@honolulu.gov
County of Hawaii	Diane Nakagawa	961-8440	n/a	Diane.Nakagawa@hawaiicounty.gov
Hawaii County Council	Diane Nakagawa	961-8440	n/a	Diane.Nakagawa@hawaiicounty.gov
County of Hawaii - Department of Water Supply	Ka'iulani L. Matsumoto	961-8050 ext. 224	961-8657	kmatsumoto@hawaiidws.org
County of Maui	Jared Masuda	463-3816	n/a	jared.masuda@co.maui.hi.us
Maui County Council	Marlene Rebugio	270-7838	n/a	marlene.rebugio@mauicounty.us
County of Maui - Department of Water Supply	Ashley Decastro	270-7680	270-7136	ashley.decastro@co.maui.hi.us
County of Kauai	Ernest Barreira	241-4295	241-6297	ebarreira@kauai.gov
Kauai County Council	Codie Tabalba	241-4193	241-6349	ctabalba@kauai.gov
County of Kauai - Department of Water	Christine Erorita	245-5409	245-5813	cerorita@kauaiwater.org

USE OF PRICE & VENDOR LIST CONTRACTS BY NONPROFIT ORGANIZATIONS. Pursuant to HRS §103D-804, nonprofit organizations with current purchase of service contracts (HRS chapter 103F) have been invited to participate in the SPO price & vendor lists contracts.

A listing of these nonprofit organizations is available at the SPO website: http://spo.hawaii.gov. Click on *For Vendors > Non-Profits > Cooperative Purchasing Program > View the list of qualifying nonprofits eligible to participate in cooperative purchasing.*

If a nonprofit wishes to purchase from a SPO price or vendor list contract, the nonprofit must obtain approval from each Contractor, i.e., participation must be mutually agreed upon. A Contractor may choose to deny participation by a nonprofit. Provided, however, if a nonprofit and Contractor mutually agree to this arrangement, it is understood that the nonprofit will retain its right to purchase from other than a SPO price or vendor list Contractor(s).

CONTRACTORS. The authorized contractors are listed in this price list contract. They have signed a Master Agreement with the State of Idaho and a Participating Addendum with the Hawaii State Procurement Office.

Contractor:	Master Agreement Number:
22nd Century Technologies Inc.	MA2025001
Cogent Infotech Corporation	MA2025003
Global Solutions Group Inc.	MA2025005
Qlogic, LLC	MA2025010

VENDOR CODES for annotation on purchase orders are obtainable from the *Alphabetical Vendor Edit Table* available at your department's fiscal office. Agencies are cautioned that the remittance address on an invoice may be different from the address of the vendor code annotated on the purchase order.

COMPLIANCE PURSUANT TO HRS §103D-310(c). Prior to awarding this contract, the SPO verified compliance of the Contractor(s) named in the SPO Price List Contract No. 26-09. *No further compliance verification is required prior to issuing a contract, purchase order, or pCard payment when utilizing this contract.*

PURCHASING CARD (pCard). The State of Hawaii Purchasing Card (pCard) is required to be used by the Executive department/agencies, excluding the DOE, SFA, HHSC, OHA, and UH, for orders totaling less than $2,500. For purchases of $2,500 or more, agencies may use the pCard, subject to its credit limit, or issue a purchase order.

PURCHASE ORDERS may be issued for purchases of $2,500 or more and for vendors who either do not accept the pCard, or set minimum order requirements before accepting the pCard.

SPO VL CONTRACT NO. 26-09 & applicable **NASPO VALUEPOINT MASTER AGREEMENT NUMBER** shall be typed on purchase orders issued against this price list contract**.** For pCard purchases, the SPO Price List Contract No. 26-09 and the applicable NASPO ValuePoint Master Agreement Number shall be notated on the appropriate transaction document.

PAYMENTS are to be made to the Contractor(s) remittance address. HRS §103-10 provides that the State shall have thirty (30) calendar days after receipt of invoice or satisfactory completion of contract to make payment. Payments may also be made via pCard.

LEASE AGREEMENTS are allowed under this contract.

STATE GENERAL EXCISE TAX (GET) AND COUNTY SURCHARGE shall not exceed the following rates if seller elects to pass on the charges to its customers.

COUNTY	COUNTY SURCHARGE TAX RATE	STATE GET	MAX PASS-ON TAX RATE	EXPIRATION DATE OF SURCHARGE TAX RATE
C&C OF HONOLULU	0.50%	4.0%	4.7120%	12/31/2030
HAWAII	0.50%	4.0%	4.7120%	12/31/2030
COUNTY OF MAUI (including Molokai and Lanai)	0.50%	4.0%	4.7120%	12/31/2030
KAUAI	0.50%	4.0%	4.7120%	12/31/2030

The GET or use tax and county surcharge may be added to the invoice as a separate line item and shall not exceed the current max pass-on tax rate(s) for each island.

County surcharges on state general excise (GE) tax or Use tax may be visibly passed on but is not required. For more information on county surcharges and the max pass-on tax rate, please visit the Department of Taxation's website at http://tax.hawaii.gov/geninfo/countysurcharge.

COMPLIANCE PURSUANT TO HRS §103-53. All state and county contracting officers or agents shall withhold final payment of a contract until the receipt of tax clearances from the director of taxation and the Internal Revenue Service. This section does not apply to contracts of less than $25,000.

VENDOR AND PRODUCT EVALUATION form, SPO-012, for the purpose of addressing concerns on this vendor list contract, is available to agencies at the SPO website: http://spo.hawaii.gov. Click on *Forms* on the home page.

PRICE OR VENDOR LIST CONTRACT AVAILABLE ON THE INTERNET at the SPO website: http://spo.hawaii.gov. Click on *Price & Vendor List Contracts* on the home page.

EMERGENCY PURCHASE. The FEMA special provisions have been added to the contact to allow departments/agencies to make purchases during a declared disaster and seek FEMA reimbursement during a declared emergency. For more information, please visit: https://spo.hawaii.gov/for-state-county-personnel/disaster-preparedness-procurement/fema-reimbursement/

The following Contractors have agreed to the FEMA special provisions:

- 22nd Century Technologies Inc.
- Global Solutions Group Inc.
- Qlogic, LLC

CONTRACT INFORMATION

Definitions

- Active Participant: An Eligible Person that voluntarily elects to activate their participation by agreeing to use the Notification and Credit Monitoring Services.
- Breach or Data Breach: A security incident in which sensitive, protected or confidential Data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
- Breach Response Specialist: A specialized role, performed by an attorney, in responding to a Data Breach or other cyber incident.
- Data: All information developed, documented, derived, stored, installed, or furnished by the Purchasing Agency under a Participating Addendum, including all information related to records owned by or in the possession of the Purchasing Agency. (Data may include PII, PHI, etc.)
- Eligible Person: Every individual or business that meets the criteria established by a Participating Agency to qualify for the Notification and Credit Monitoring Services. The Participating Agency will have sole discretion to determine who qualifies as an Eligible Person.
- Event: Any observable occurrence in a network or system.
- Incident, Cyber Security Incident, or Security Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices in order to affect a system, application, or network's integrity or availability and/or the unauthorized access or attempted access to a system or systems.
- Incident Manager: The individual who manages the process to restore normal service operation as quickly as possible to minimize the impact to business operations. Responsible for planning and coordinating all the activities required to perform, monitor, and report on the process.
- Personally Identifiable Information or PII: Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
- Threat: The potential source of an adverse event; the possibility of a malicious attempt to damage or disrupt a computer network or system.
- Triggering Event: A Breach or suspected Breach of PII, or any other circumstance which results in a Participating Agency activating Notification and Credit Monitoring Services under the Master Agreement (through a Participating Addendum).
- Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

General Requirements (applies to all categories)

1. Security of Information. Protection of Data must be an integral part of the business activities of the Contractor to ensure that there is no inappropriate or unauthorized use of Data at any time. To this end, the Contractor must safeguard the confidentiality, integrity, and availability of Data and comply with the following conditions: All Purchasing Agency Data obtained by the Contractor must become and remain property of the Purchasing Agency. At no time shall any Data or processes which either belong to or are intended for the use of the Purchasing Agency or its officers, agents, or employees, be copied, disclosed, or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Agency. The Contractor must meet or exceed the requirements of the Purchasing Agency's security

policies, standards, and regulatory and contractual obligations as defined in the Purchase/Work Order. The Contractor must have security measures in place to ensure that a Purchasing Agency's sensitive or protected information and/or Data at rest, in use, or in transit is not compromised through a Breach of the Contractor's system and/or applications.

2. The Contractor must notify the Purchasing Agency of any suspected or actual Breach of the Purchasing Agency's or Active Participants' Data immediately upon discovery.
3. The Contractor must ensure all services are performed by trained experts in the field relevant to the services ordered, who possess the experience and qualifications identified in the Contractor's response.
4. The Contractor must be AICPA SOC 2 compliant covering all 5 functional areas (Security, Availability, Processing Integrity, Confidentiality, and Privacy), or a third-party assessment based on current revision of NIST 800-53 Moderate controls conducted with in the last two years, or FedRAMP authorization, or GovRAMP authorization. This is a mandatory requirement. The Contractor must keep all information regarding the Purchasing Agency, Eligible Persons and Active Participants, whether obtained from the Purchasing Agency, from Eligible Persons, or through performance of the services under the Master Agreement, confidential and secure and additionally must dispose of all information in a manner that meets or exceeds the AICPA SOC 2 standards.
5. The Contractor must contact the Purchasing Agency immediately upon receipt of any electronic discovery, litigation holds, discovery searches, expert testimony, or other similar requests which in any way might reasonably require access to the Purchasing Agency's Data.
6. The Contractor must not respond to subpoenas, service of process, and other legal requests related to the Purchasing Agency without first notifying the Purchasing Agency unless prohibited by law from providing such notice.
7. The Purchasing Agency owns all rights, title and interest in its Data that is related to the services provided under any Order. The Contractor must not access the Purchasing Agency's user accounts or Data, except (i) in the response to service or technical issues, (ii) as required by the express terms of the Order, or (iii) at the Purchasing Agency's written request.
8. Orders: A Purchasing Agency may customize services ordered. The Contractor must maintain the ability to provide all services available under this Category throughout the entire Master Agreement term, including all renewals. The Purchasing Agency will work with the Contractor to develop a Statement of Work for each Order. A Purchasing Agency may elect to use a limited selection of services rather than all services available under this Category. For example, a Purchasing Agency may elect to evaluate threats and vulnerabilities in their current environment but not utilize training services. The Purchasing Agency reserves the right to amend any Order.
    a. The Purchasing Agency will provide a Statement of Work which will include a detailed task list, deliverables, timeframes, estimated level of effort and staffing levels for the specific services.
    b. If the service is to be performed on-site, travel costs will be reimbursed in accordance with the Purchasing Agency's travel policy, which will be included with the Order.
9. The Contractor must work collaboratively with the Purchasing Agency and produce relevant, accurate documents that use terminology that is easily understood by a layperson.
10. All call centers provided under the Master Agreement(s), including the call center personnel themselves when providing services under the Master Agreement(s), must remain within the contiguous United States. While remaining compliant with that, call

center personnel may work off-site. Contractor staff must be able to communicate plainly and clearly in English in a manner that can be easily understood by customers.

Category 1 – Risk Assessment and Mitigation Services

Risk assessment and mitigation services: professional services that help organizations identify potential risks, evaluate their likelihood and impact, and then develop strategies to minimize or eliminate those risks, essentially protecting the organization's assets and ensuring business continuity by proactively addressing potential threats; it involves both analyzing potential dangers and taking proactive steps to manage them effectively.

- Risk identification: Identifying potential hazards and threats that could affect the organization, including internal and external factors.
- Risk analysis: Evaluating the likelihood and severity of each identified risk, often using qualitative or quantitative methods.
- Risk prioritization: Ranking risks based on their potential impact and likelihood of guiding mitigation efforts.
- Mitigation strategy development: Creating actionable plans to address each identified risk, including preventive measures, contingency plans, and risk transfer options.
- Implementation and monitoring: Putting mitigation strategies into practice and regularly reviewing their effectiveness to adapt to changing circumstances.

General Requirements

1. Data Encryption and Data Location Requirements. Non-Public Data: All Non-Public Data (includes PII and any other Data that the Purchasing Agency requires to be protected) provided by a Purchasing Agency to the Contractor must be encrypted at rest and in transit with controlled access. Unless otherwise provided in the Purchasing Agency's Purchase Order, the Contractor is responsible for encryption of the Non-Public Data. All encryption shall be consistent with validated cryptography standards such as the current standards in FIPS 140-2, Security Requirements for Cryptographic Modules, or the then-current NIST recommendation. All Data shall be considered Non-Public Data by the Contractor unless the Purchasing Agency has identified Data it deems as Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the Purchasing Agency's Purchase Order.
2. Data Location: Any data centers used by the Contractor for activities related to the services required must be located within the Continental United States and storage of Data at rest shall be located solely in data centers located within the Continental United States. The Contractor shall not allow its personnel or subcontractors to store Data on portable devices, except for devices that are used and kept only at its data centers located within the Continental United States. Each data center used by the Contractor must be within a physical security perimeter to prevent unauthorized access, and physical entry controls must be in place so that only authorized personnel have access to Data.

Services

1. The Contractor must perform vulnerability assessments, privacy impact and policy assessments, and evaluation and analysis of internal controls critical to the detection and elimination of vulnerabilities to the protection of Data, as defined by a Purchasing Agency. Services include, but are not limited to:

- Implementation of risk assessments and mitigation strategies in alignment with published, mainstream information security frameworks and standards.
- Compliance assessment of the Purchasing Agency's disclosure responsibilities for Data. This includes compliance with applicable federal, state, and local regulations, and standards governing the protection of information.
- Evaluation of threats and vulnerabilities to Data in the Purchasing Agency's current environment, including any proprietary systems.
- Prioritization of threats and weaknesses identified by an assessment and cost evaluation.
- Review of, and recommendations for the improvement and/or creation of information security policies.

2. The Contractor must design and develop business processes, procedures, and business applications in response to risk assessments.
3. The Contractor must provide a comprehensive final written report within one (1) week of conclusion of the engagement (or as otherwise determined by the Purchasing Agency) that at a minimum includes detailed risk statements, explanations, and recommendations for mitigating identified risks.
4. Upon request by the Purchasing Agency, the Contractor may be asked to provide consultation services for development of terms for third-party contracts, including those with cloud-based providers.

Personnel Qualifications.

The roles below define the minimum qualifications that the role must have for the work performed under this category.

1. Security/Technology Senior Analyst: 5+ years of professional experience. Strong technical and/or security skills. Experienced in specific areas, relative to the project. Able to plan and coordinate the technical tasks and work necessary for delivery of services. Able to design and oversee completion of deliverables. Can manage and coach staff and provide QA over the process and work product, as it relates to risk, security and/or technical matters. Strong communications, analysis skills, troubleshooting, and issue resolution skills. Security or technology certification.
2. Business Process/ Risk Management Senior Consultant: 5+ years of professional experience. Deep knowledge of business processes, industry issues, and/or risk management. Understands big picture and able to prioritize issues, based on data discovery and experience. Can provide recommendations related to security and technology matters. Able to supervise large and diverse teams and provide QA over the process and work product. Often serves as a technical subject matter specialist. Strong communication and facilitation skills.
3. Project Manager: 5+ years of professional experience. Project Management and Business process subject matter experts. Skills and experience in managing engagement work efforts, scoping and assigning work, and managing engagement budgets. Tracks and communicates project status and demonstrates project value. Project management certification.

Category 2 – Incident Response Services

All incident response services must be carried out by trained experts and meet all legal standards. Incident response services assist organizations in detecting, containing, and mitigating damage from cybersecurity breaches or attacks, essentially providing a rapid response to security incidents to minimize harm and restore system functionality when a threat occurs; they aim to identify, analyze, and address security issues quickly, while also learning from past incidents to improve future preventative measures.

Key points about incident response services:

- Function: When a security breach happens, the incident response team is activated to manage the situation, including isolating the threat, investigating its origin, and taking steps to prevent further damage.
- Benefits:
  - Expertise: Access to specialized cybersecurity professionals who can handle complex threats.
  - Rapid response: Quick identification and containment of incidents, minimizing potential damage.
  - Improved security posture: Analysis of incidents to identify vulnerabilities and implement preventative measures.
- Typical services:
  - Threat detection and analysis
  - Incident containment and eradication
  - Data recovery and restoration
  - Forensics investigation
  - Post-incident reporting and improvement planning

Service Initiation/Customer Service/ Consultants

1. Orders. A Purchasing Agency may customize services ordered. The Contractor must maintain the ability to provide all services available under this Category throughout the entire Master Agreement term, including all renewals. The Purchasing Agency will work with the Contractor to develop a Statement of Work for each Order. A Purchasing Agency may elect to use a limited selection of services rather than all services available under this Category. The Purchasing Agency reserves the right to amend any Order to add or remove services as the actual scope of the Event or Incident is determined.
    a. The Statement of Work must include a detailed task list, deliverables, timeframes, estimated level of effort and staffing levels for the specific services.
    b. If the service is to be performed on-site, travel costs will be reimbursed in accordance with the Purchasing Agency's travel policy, which will be included with the Order.
2. The Contractor must provide timely response to a Purchasing Agency's request for services. The Contractor must maintain an active, monitored email account for priority or urgent communications.
3. After initial request is transmitted by the Purchasing Agency to the Contractor's representative, an Incident Manager must respond by telephone or email within four (4) hours.
4. If the Incident requires an on-site Contractor presence, the Contractor must be on-site within one (1) business day of request, or as mutually agreed on the Order.
5. The Contractor must ensure all Consultant services are performed by trained experts in the field relevant to the services ordered, who possess the experience and qualifications identified in the Contractor's response.

Event and Incident Management

1. The Contractor must work with the Purchasing Agency to determine the actual scope of an Event and determine if the Event is an Incident. This may include, but is not limited to, gathering information from various sources such as log files, error messages, and other resources such as intrusion detection systems and firewalls that may produce evidence to determine if an Event is an Incident.
2. The Contractor must collect evidence, follow Chain of Custody protocol, and document all actions taken during the Event or Incident Response.
    a. All Event and Incident documentation must be made available to the Purchasing Agency and law enforcement upon request.
3. The Contractor must identify when the Purchasing Agency should contact law enforcement, and the Contractor must work with law enforcement under the direction of the Purchasing Agency.
4. Because of the sensitive and confidential nature of information and communication surrounding an Incident, the Contractor must ensure all communication is through secure channels and disclosure of Incident information is limited to identified Purchasing Agency personnel and limited to a need-to-know basis (as defined by the Purchasing Agency) for all others.
5. Containment Services. The Contractor shall provide containment services that include but are not limited to:
    a. Short-term containment of an Event or Incident to limit the damage incurred while preventing the destruction of any evidence that may be needed for later prosecution.
    b. System back-up utilizing forensic software that preserves evidence and captures affected system(s) as they were during the Incident.
    c. Long-term containment of affected system(s) to allow systems to be used in production during eradication.
6. Eradication Services. The Contractor shall provide eradication services that include but are not limited to: Removal of malicious or illicit code and restoration of affected system(s).
7. Recovery Services. The Contractor shall provide recovery services that include but are not limited to: Reinstatement of affected system(s) into the production environment. May include, but is not limited to testing, monitoring, and validation that ensure reinstated system(s) do not re-infect the environment and are not otherwise compromised.
8. Forensic Analysis. The Contractor shall conduct forensic analysis that includes but is not limited to:
    a. In-depth analysis or investigation and report that objectively identifies and documents the culprits, reasons, course, and consequences of a security incident, utilizing a legally admissible methodology. Services include, but are not limited to the following:
        i. Protect the system during forensic examination from any possible alteration, damage, corruption of Data, or virus introduction.
        ii. Discover and recover all files on the system, including but not limited to existing normal, deleted, hidden, password-protected, and encrypted files; reveal the contents of hidden, temporary, and swap files; access the contents of protected or encrypted files, if possible and legally appropriate; and analyze all possibly relevant Data, including Data found in unallocated space on a disk and slack space in a file.
        iii. Create report that includes overall analysis of the subject system, all

possibly relevant files, and discovered file Data. Report may include, but is not limited to system layout, file structures, any Data and authorship information discovered, any attempts to hide, delete, protect, and encrypt information, and any other discovered information or Data that appears to be relevant to the examination. The report must be provided within the timeframe specified by the Purchasing Agency.

iv. Provide expert consultation and/or testimony, when required by the Purchasing Agency.

9. Reporting
    a. The Contractor must provide comprehensive reviews and analyses of a Purchasing Agency's Event or Incident. Reports may include, but are not limited to:
        i. Review and report that includes identification of potentially compromised information, trends, and unusual patterns.
        ii. Investigation and report of the circumstances surrounding the Event or Incident, including determination of whether or not the Event or Incident appears to be incidental, accidental, or targeted.
        iii. Analysis of the compromised Data to determine if there is evidence of Data mismanagement or compromise.
        iv. Report that includes aggregate and complete information to date, allowing the Purchasing Agency to quickly address inquiries from Federal, state, and local stakeholders and the media.
        v. Post-incident analysis that identifies necessary improvements to existing security controls and practices and includes recommendations for correcting systemic weaknesses and deficiencies in policies and procedures.
    b. During the engagement, reports must be incrementally delivered on a schedule defined by the Purchasing Agency. This includes, but is not limited to:
        i. Written status reports of activities completed, findings, and planned activities no less frequently than weekly or as otherwise determined by the Purchasing Agency.
        ii. Comprehensive final written report within one (1) week of conclusion of the engagement, or as otherwise determined by the Purchasing Agency.
        iii. Written inventory of all copies made of files or configurations from workstations, servers, or network devices.
        iv. Executive briefings and written summaries, as appropriate to the Incident or Event.
10. 24x7 Customer Support
    a. The Contractor must provide customer support that may be reached via toll free number 24x7, every day of the year.
    b. The Contractor must clearly identify to callers the method to access services for each distinct Triggering Event.
    c. Staff must answer questions regarding services, eligibility, and enrollment in a courteous and professional manner, using the FAQ script, if one is provided by the Purchasing Agency. Additionally, all calls must be answered by a member within one (1) minute of the call being placed.
11. Personnel Qualifications. The roles below define the minimum qualifications that the role must have for the work performed under this category.
    a. Forensics Incident Investigator: 5+ years of professional experience. Subject matter expertise in identifying, collecting, examining, and preserving digital

evidence using controlled and documented analytical and investigative techniques. Forensics certification.

b. Business Process/ Risk Management Senior Consultant: 5+ years of professional experience. Deep knowledge of business processes, industry issues, and/or risk management. Understands big picture and able to prioritize issues, based on data discovery and experience. Can provide recommendations related to security and technology matters. Able to supervise large and diverse teams and provide QA over the process and work product. Often serves as a technical subject matter specialist. Strong communication and facilitation skills.
c. Project Manager: 5+ years of professional experience. Project Management and Business process subject matter experts. Demonstrated experience in Information Security Incident Response Services. Skills and experience in managing engagement work efforts, scoping and assigning work, and managing engagement budgets. Tracks and communicates project status and demonstrates project value. Project management certification.

Category 3 – Breach Coach Services

Data breach coaching services involve specialized guidance and support for businesses experiencing or at risk of a cybersecurity incident, offered to help navigate the incident response process and mitigate potential damages. Please note: Any and all legal services on behalf of the Purchasing Agency must be approved by Purchasing Agency at the time the Work Order is executed, some Purchasing Agencies may require additional internal approval of any outside legal services.

1. Service Initiation/Customer Service/Breach Response Specialists
    a. Orders. A Purchasing Agency may customize services ordered. The Contractor must maintain the ability to provide all services available under this Category throughout the entire Master Agreement term, including all renewals. The Purchasing Agency will work with the Contractor to develop a Statement of Work for each Order. A Purchasing Agency may elect to use a limited selection of services rather than all services available under this Category. The Purchasing Agency reserves the right to amend any Order to add or remove services as the actual scope is determined.
        i. The Statement of Work must include a detailed task list, deliverables, timeframes, estimated level of effort and staffing levels for the specific services.
        ii. If the service is to be performed on-site, travel costs will be reimbursed in accordance with the Purchasing Agency's travel policy, which will be included with the Order.
    b. The Contractor must provide timely response to a Purchasing Agency's request for services. The Contractor must maintain an active, monitored email account for priority or urgent communications.
    c. After initial request is transmitted by the Purchasing Agency to the Contractor, the Contractor must respond by telephone or email within two (2) business days.
    d. The Contractor must provide the required services within one (1) business day of request, or as mutually agreed on the Order.
    e. The Contractor must ensure all Breach Response Specialists that provide services are trained experts in the field relevant to the services ordered, who

possess the experience and qualifications identified in the Contractor's response.

2. The Contractor must provide guidance, advice and consultation to coordinate and support the Purchasing Agency's Breach response, including the investigation and mitigation of a Breach impacting individuals or organizations that may be located within the state, region, or dispersed nationwide. Services may include, but are not limited to:
    a. Work collaboratively with the Purchasing Agency's incident response team and Incident response Contractor, if applicable. The Contractor must also cooperatively and collaboratively engage with internal stakeholders such as, but not limited to, the Purchasing Agency's legal counsel, state's attorneys general, federal regulators, internal IT and Human Resources staff, Risk Management, and public relations/media representative(s) as appropriate to the Breach.
    b. Facilitate Crisis Management that arises from the Breach by engaging and collaborating with external partners such as Public Relations firms, IT consultants, Forensic Accountants, and Credit Monitoring and Notification services providers, and law enforcement.
    c. Determine whether the Data compromised by a Breach requires notification, as defined by state and Federal security breach laws.
    d. Advise on communication strategy and notification requirements, including, but not limited to, preparing and supporting communications regarding the Breach to regulators, affected individuals, the media, and others identified by the Purchasing Agency.
    e. Provide counsel on ethical implications, reputation management, and the subsequent risks following any Data Breach.
    f. Advise on legal consequences and rules applicable to the Purchasing Agency's compliance with relevant data protection laws.
    g. Assist the Purchasing Agency during regulatory investigation, litigation or both.
3. Personnel Qualifications. The role below defines the minimum qualifications that the role must have for the work performed under this category.
    a. Breach Coach: 5+ years of professional experience. Subject matter expertise in assisting organizations navigate their cyber response and recovery to include isolating affected data, incident breach reporting requirements, notifying customers, retaining necessary forensics professionals and managing crisis communications. Demonstrated knowledge in building an incident response plan, developing cyber security awareness programs and facilitating other efforts to help minimize risk.

Category 4 – Notification and Credit Monitoring Services

1. Service Activation
    a. A Purchasing Agency may decide, in its sole discretion, to begin using the services described in the Master Agreement for Category 4 at any time during the term of the Master Agreement.
    b. Orders. A Purchasing Agency may customize services ordered. The Contractor must maintain the ability to provide all services available under this Category throughout the term of the Master Agreement. A Purchasing Agency may elect to use a limited selection of services rather than all services provided under this Category. For example, a Purchasing Agency may activate Call Center and Credit Monitoring and Identity Theft Monitoring services but not

Notification services.

c. Each Purchasing Agency has sole discretion to determine if and when it will activate services and to define the eligibility requirements for Eligible Persons to register for the services provided under the Master Agreement.
d. Activation of services shall commence upon written notification to the Contractor by a Purchasing Agency.
    i. The Purchasing Agency will provide the Contractor with a list of apparent Eligible Persons as detailed in section Notifications below.
    ii. The Purchasing Agency may provide a Frequently Asked Question (FAQ) script to ensure the Contractor's staff provide consistent responses to inquiries about a Triggering Event. When an FAQ is provided by the Purchasing Agency, the Contractor shall direct its staff in its use.

2. Notifications
    a. The Contractor must meet each state's unique rules governing the need to notify affected persons of Triggering Events, including content and timing requirements.
    b. Upon issuance of an Order, the Contractor must work with each Purchasing Agency to develop a sample Scope of Work Notification Plan (Notification Plan) and template based on each Purchasing Agency's requirements in order to facilitate timely notification in the event of a Triggering Event.
        i. The Notification Plan may include information including but not limited to:
            1. An overview of the Purchasing Agency's requirements;
            2. A general timeline for the Purchasing Agency notifying the Contractor of the Triggering Event, the Purchasing Agency providing information to the Contractor, and the Purchasing Agency determining whether or not the Contractor will send notifications to affected persons;
            3. A notification template that the Contractor may use to develop notices to send to affected persons, or to customize for a specific Triggering Event, at the option of the Purchasing Agency;
            4. A general timeline for the Purchasing Agency approving the draft notification and the Contractor sending the notifications; and
            5. The Purchasing Agency's selected method of sending notifications.
        ii. The Notification Plan and template must be approved by the Purchasing Agency. If a Triggering Event occurs prior to the development and approval of a Notification Plan and template, the Contractor must immediately work with the Purchasing Agency to develop the Notification Plan within 72 hours. If a Triggering event has not yet occurred, a Notification Plan must be developed within 30 days of a signed Order.
    c. Upon notification by a Purchasing Agency that a Triggering Event has occurred which requires notifications, and at the option of the Purchasing Agency, the Contractor must intake, review, and data cleanse the Purchasing Agency - furnished data set of identified apparent Eligible Individuals which includes but is not limited to review of National Change of Address (NCOA).
        i. The Contractor shall remove repetitive information for the same

individual (de-duplicate the Data) and provide a final notification list and a duplicate list (names removed during the de-duplication process) to the Purchasing Agency for approval within seven (7) calendar days of receipt of the data set and prior to sending notifications.

d. Upon notification by a Purchasing Agency that a Triggering Event has occurred which requires notifications, and at the option of the Purchasing Agency, the Contractor must prepare, print (if notification by mail is ordered), and send all notifications via the delivery method specified by the Purchasing Agency.
    i. The Purchasing Agency shall provide written approval of any notice prior to it being sent.
    ii. The Purchasing Agency shall approve the final notification list (if data cleansing is ordered by the Purchasing Agency) or otherwise provide a list of names and address, in Microsoft Excel or another mutually agreeable file format, of persons to whom the notification must be sent.
    iii. The Contractor must send notifications within the timeframe required by the Purchasing Agency's laws and regulations.
e. The Contractor shall only use the contact information provided by the Purchasing Agency to send the required notifications, unless the Purchasing Agency agrees in writing to allow the Contractor to send additional materials or make additional contact.

3. "Codes Only" Reduced Scope Service. The Contractor must also provide, as an alternative to full enrollment in the services described in sections above, a "codes only" reduced scope service (triple bureau) in which the Contractor issues a list of PINs (unique activation codes) upon request by a Participating Entity, which can be used by Eligible Persons on a per-occurrence basis. The PINs must be valid for redemption for a minimum of ninety (90) calendar days from the date of issuance. Eligible Persons must have the option to enroll online via the Contractor's website, or offline via toll free telephone number.
4. Call Center
    a. The Contractor must provide a call center that may be reached via toll free number 24x7, every day of the year.
    b. The Contractor must clearly identify to callers the method to access services for each distinct Triggering Event.
    c. Staff at the call center must answer questions regarding services, eligibility, and enrollment in a courteous and professional manner, using the FAQ script, if one is provided by the Purchasing Agency. Additionally, all calls to the call center must be answered by a call center staff member within one (1) minute of the call being placed.
5. Customer Service
    a. The Contractor must provide the highest quality of customer service to each Eligible Person and Active Participant. All customer service representatives must treat all Eligible Persons and Active Participants with respect and offer assistance in resolving any issues, concerns, or complaints.
    b. If the customer service representative cannot adequately address the concerns of an Eligible Person or Active Participant, the concern must be elevated according to the agreed-upon Service Level Agreement (SLA).
    c. The Contractor must, at a minimum, provide the following:
        i. Resources to assist Eligible Persons and Active Participants in a manner consistent with the agreed-upon SLA; and
        ii. Call centers and customer support personnel located within the United States.

6. Reporting
    a. Monthly Usage Reports. The Contractor must provide monthly usage reports to each Purchasing Agency that has activated services, in a format acceptable to the Purchasing Agency. Information that must be contained within usage reports includes but is not limited to the following:
        i. Number of Active Participants (including type of service);
        ii. Aggregate count of Active Participants;
        iii. Number of credit monitoring alerts issued by type;
        iv. Number of identity theft alerts issued by type;
        v. Number and types of corrective action(s) taken for identify theft protection and identity theft resolution (if applicable);
        vi. Number of telephone calls from either Eligible Persons or Active Participants (separately identified) answered by the Contractor's call centers;
        vii. Average "wait time" experienced by callers before speaking to the Contractor's representatives; and
        viii. Number of identity theft insurance claims filed by Active Participants (if applicable).
    b. Ad Hoc Reporting. Upon request by the Purchasing Agency, the Contractor must provide ad hoc reporting. Unless prohibited by law, requested data may include, but is not limited to names, addresses, and email addresses of Active Participants.
7. Credit Monitoring. Upon request by the purchasing entity, the Contractor may be asked to provide the following services to all Active Participants:
    a. Enrolling Eligible Persons
        i. When a Purchasing Entity notifies the Contractor to activate services, the Purchasing Agency will provide a list including names and addresses of all Eligible Persons.
        ii. The Contractor must begin enrolling Eligible Persons who choose to become Active Participants as soon as it receives the list described in the section above.
        iii. At a minimum, the Contractor must provide Eligible Persons the option to enroll by phone, mail, and online.
        iv. The Contractor shall not require Active Participants to provide any information beyond the information typically required and reasonably necessary to provide the contracted services.
        v. The Contractor shall not automatically subscribe or enroll Active Participants in follow-on services, require Active Participants to enroll in follow-on services, or imply that follow-on services are otherwise required by Active Participants. Follow-on services are any additional services offered by the Contractor that are not included in the Master Agreement or Participating Addendum.
        vi. The Contractor must terminate services to each Active Participant at the end of each Enrollment Term as defined in section 5.7.2. There must not be an automatic renewal of the service to the Active Participant. The Contractor must notify each Active Participant in writing of the upcoming service termination no later than one (1) month before the expiration of the Enrollment Term.
    b. Enrollment Term. Eligible Persons that elect to become Active Participants shall receive Credit Monitoring, Identity Theft Monitoring and alerts/notifications for a period of one (1) year. The Purchasing Agency may

elect to provide Active Participants services for additional period(s) of not less than one (1) year each. Upon the expiration of the Enrollment Term between the Contractor and an Active Participant, the Contractor must dispose of all the Active Participant's information by a secure method.

c. Credit Monitoring. The Contractor must provide daily monitoring of one (1) or three (3) of the three (3) major credit bureaus, depending on the level of services elected by the Purchasing Agency. The Contractor must monitor for activity including, but not limited to, new lines of credit and credit inquiries.
d. Identity Theft Monitoring. The Contractor must provide monitoring designed to detect theft of an Active Participant's identity. Examples of such monitoring include but are not limited to: monitoring of new accounts, public records, address changes, non-credit/payday loans, and scanning of underground/black market websites for use of protected information.
e. Alerts/Notifications. The Contractor must provide alerts/notifications to Active Participants related to anomalous or suspicious activities identified by the Contractor through the Contractor's Credit Monitoring and Identity Theft Monitoring. The Contractor must notify Active Participants via the notification method identified by the Active Participant within twelve (12) hours of identifying the activity.
f. Identity Theft Restoration Assistance. The Contractor must provide identity theft restoration assistance to any Active Participant who becomes a victim of identity theft while enrolled in Credit Monitoring and Identity Theft Monitoring services, even if the identity theft is not discovered until after the Credit Monitoring and Identity Theft Monitoring services have expired. At a minimum, the Contractor must:
    i. Provide access to a contact center available 24x7, every day of the year, that can provide identity theft resolution customer care services. Individuals staffing this contact center must be trained and experienced in assisting customers with understanding their credit reports and restoring their credit; automated responses will not satisfy this requirement.
    ii. Review occurrences of identity theft and provide an initial course of action within forty-eight (48) hours of the report of the occurrence.
    iii. Provide one-on-one counseling to assist Active Participants with resolving any identity theft problems, such as contacting the Active Participant's creditors and others in order to resolve the identity theft problem on the Active Participant's behalf.
    iv. Continue providing restoration assistance until the Contractor and Active Participant agree that the identity theft issues have been resolved or the Contractor has exhausted the insurance policy (if applicable).

8. Category 4: Value Added Services: Identity Theft Insurance. Optional Services to be used at the direction of the Participating Agency, the Contractor must provide insurance to all Active Participants for loss due to identity theft, which meets the following minimum requirements:
    a. Not less than one million dollars ($1,000,000) in coverage for each Active Participant.
    b. Coverage for at least the following losses which result solely from the theft of the individual's identity:
        i. Costs associated with re-filing applications including but not limited to loan applications and grants applications that were denied because of

the identity theft.

ii. Costs for notarizing affidavits, long-distance calls, and postage required to restore the individual's identity.

iii. Costs for six (6) credit reports within the twelve (12) months following the theft.

iv. Lost wages resulting from the need to take time off from work in order to engage in identity restoration activities. Lost wages include reimbursement of paid time off (e.g. vacation, annual leave, etc.) taken for the purpose of engaging in identity restoration activities.

v. Legal fees incurred in the defense of a civil suit against the Active Participant for non-payment, which suit resulted from the identity theft, or for removal of a judgment against the Active Participant that resulted from the identity theft.

c. In the event the Contractor's underlying policy for identity theft insurance is terminated, the Contractor must notify all Active Participants and must have another policy of equal value in place immediately upon termination to ensure that no coverage gaps exist.

d. Identity theft insurance requirements extend to any identity theft that occurs while the Active Participant is enrolled, even if the identity theft is not discovered until after the Credit Monitoring and Identity Theft Monitoring services have expired.

AGENCY INSTRUCTIONS

1. For Executive Departments Only. Purchasing Agency is required to contact their IT Coordinator for instructions and assistance with procuring Cybersecurity and Information Security Services from one of the authorized contractors listed in Price List Contract No. 26-09. Prior approval for all procurements using this Price List is required by the Purchasing Agency's IT Coordinator.
2. For Executive Departments Only. Prior approval for IT related service is required to be submitted to ETS IT Governance by the IT Coordinator, via the ETS IT Spend Request process.
3. Purchasing Agency shall issue a Statement of Work (SOW) to the authorized vendor(s). The Purchasing Agency shall obtain one (1) price quote from one of the authorized vendors for procurements up to $50,000. For procurements more than $50,000, two (2) or more price quotes shall be solicited from two (2) different authorized vendors and provided the SOW.

    - For Categories 1-3: At minimum, a SOW shall include a detailed task list, deliverables, timeframes, estimated level of effort and staffing levels for the specific services. If the services it to be performed on-site, travel costs will be reimbursed in accordance with the agency's travel policy which will be included with the order.
    - For Category 1: The Purchasing Agency shall identify Data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the Purchasing Agency's Purchase Order.
    - For Category 4: Each Purchasing Agency has sole discretion to determine if and when it will activate services and to define the eligibility requirements for Eligible Persons to register for the services. Activation of services shall commence upon written notification to the Contractor by a Purchasing Agency. The Purchasing Agency will provide the Contractor with a list of apparent Eligible Persons.

Contractor	Category 1	Category 2	Category 3	Category 4
22nd Century Technologies Inc	X	X	X	X
Cogent Infotech Corporation	X			
Global Solutions Group Inc	X	X	X	
Qlogic LLC	X			

4. Agencies shall ensure that task orders, statements of work, or requests for quotations include the requirement to comply with the Hawaii Electronic Information Technology Disability Access Standards. The following language shall be included when procuring information technology:

    "All electronic information technology developed or provided under this contract or procurement shall comply with the applicable requirements of the Hawaii Electronic Information Technology Disability Access Standards (Access Standards)."

5. When utilizing this price list contract, awards for Value-Add Services (e.g., consulting services pre- and post-implementation) shall not exceed $100,000.00 per year and the contract term shall not exceed three (3) years, unless requesting agencies receive written approval by the CIO.
6. The Purchasing Agency shall award based on lowest price. If the lowest price does not meet the agency's specification and operational requirements, the award may be made to the authorized vendor whose offer represents the best value to the agency with a completed form SPO-010. The completed form SPO-010 is kept in the procurement file.
7. All orders at a minimum shall include: (a) the services being delivered, (b) the place services are rendered (if applicable), (c) a billing address, (d) the name, phone number, and address of the purchasing agency representative, (e) the price per hour or other pricing elements consistent with the Master Agreement and the Contractor's proposal, (f) a ceiling amount of the order for services being ordered, and (g) The SPO Price List 26-09 and Master Agreement Number.
8. Purchasing Agency should coordinate the execution of the Purchase Order (along with supporting SOW) in the following order:
9. Contractor signs the Purchase Order;
10. CIO or CIO's designee signs the Purchase Order; and
11. Purchasing Agency's procurement officer with authority to execute contracts signs the Purchase Order.
12. Purchasing Agency retains original purchase order and supporting documents.

22ND CENTURY TECHNOLOGIES INC.
Master Agreement No. MA2025003

NASPO URL: https://www.naspovaluepoint.org/portfolio/cybersecurity-information-security-services-2025-2031/22nd-century-technologies-inc/

Sales Contact:
Reddy Bollineni
Phone: (502-488-0162
Email: cyber@tscti.com

Remittance Address:
22ND Century Technologies Inc.
825 Greensboro Dr., Ste 900
Mclean, VA 22102-4938
Vendor Code: 348742-01

COGENT INFOTECH CORPORATION
Master Agreement No. MA2025003

NASPO URL: https://www.naspovaluepoint.org/portfolio/cybersecurity-information-security-services-2025-2031/cogent-infotech-corporation/

Sales Contact:
Casey Brinkman
Phone: (469) 843-9455
Email: Casey.Brinkman@CogentInfo.com

Remittance Address:
Cogent Infotech Corp.
1035 Boyce Rd., Ste 108
Pittsburgh, PA 15241
Vendor Code: 368220-00

GLOBAL SOLUTIONS GROUP, INC.
Master Agreement No. MA2025005

NASPO URL: https://www.naspovaluepoint.org/portfolio/cybersecurity-information-security-services-2025-2031/global-solutions-group-inc/

Sales Contact:
Jay Mehta
Phone: (313) 215-1676
Email: JayM@globalsolgroup.com

Remittance Address:
Global Solutions Group Inc.
31681 Dequindre Rd.
Madison Heights, MI 48071
Vendor Code: 376604-00

QLOGIC, LLC
Master Agreement No. MA2025010

NASPO URL: https://www.naspovaluepoint.org/portfolio/cybersecurity-information-security-services-2025-2031/qlogic-llc/

Sales Contact:
Jai
Phone: (201) 409-1234
Email: jai@qlogic.io

Remittance Address:
Qlogic, LLC
5 Twin Oaks Rd
Parsippany, NJ 07054
Vendor Code: 376360-00

Main Site - https://qlogic.io/
Government Page - https://qlogic.io/government/
Cyber Security - https://qlogic.io/naspo/