

**BOARD OF WATER SUPPLY
CITY AND COUNTY OF HONOLULU
REQUEST FOR SOLE SOURCE**

DATE: February 26, 2019

TO: ERNEST Y.W. LAU, P.E.
Manager and Chief Engineer

VIA: Vicki A. Kitajima
Procurement and Specifications Specialist VI

FROM: HENDERSON NUUHIWA
Program Administrator - Information Technology Division

RE: REQUEST FOR SOLE SOURCE AWARD

Pursuant to Section 103D-306, Hawaii Revised Statutes, and Subchapter 9, Chapter 3-122 of the Hawaii Administrative Rules, I am requesting that a sole source award be approved to purchase the following:

Vendor Name & address:

Center for Internet Security, Inc.
31 Tech Valley Drive
East Greenbush, NY 12061-4134

Amount of the contract:

\$21,486.90 - Purchase Order

Term of the contract:

1 Year, invoiced annually

Prior sole source contract numbers and dates:

None

Description of the goods to be purchased:

The Center for Internet Security (CIS) Netflow/Intrusion Detection System Monitoring and Analysis Service, known as **Albert**, provides a near real-time automated process tailored to State, Local, Tribal, and Territorial (SLTT) government entities, that identifies and alerts on traditional and advanced cybersecurity network threats, facilitating rapid responses to these threats and attacks.

The CIS **Albert** sensors provide Intrusion Detection System (IDS) monitoring, along with netflow and passive DNS collection and analysis. Through its 24/7/365 Security Operations Center (SOC), CIS manages the sensor(s) to identify malicious activity, and, in accordance with escalation procedures prescribed by BWS, provides notification of malicious activity.

Explanation how the unique features, characteristics or capabilities are essential for the BWS to accomplish its work:

CIS is a nonprofit organization that operates the **Multi-State Information Sharing and Analysis Center (MS-ISAC)**, which is designated by the **U.S. Department of Homeland Security (DHS)** as the **key resource for cyber threat prevention, protection, response and recovery for the nation's SLTT government entities**. Through its state-of-the-art 24/7/365 cyber security operations center, CIS serves as a central resource for situational awareness and incident response for SLTT governments. The CIS **Albert** service is unique because of this, as well as its;

- Availability only to SLTT
- Government-specific focus tailored to SLTT government's cyber security needs.
- Correlation of data from multiple public and private partners
 - Historical log analysis performed on all logs collected for specific threats reported by partners and/or trusted third parties.
 - When a major new threat is identified, CIS will search logs for prior activity. (Traditional monitoring services only alert going forward, from the date a signature is in place. There is no "look behind" to assess what activity may have already occurred.)
- Signatures from forensic analysis of hundreds of SLTT cyber incidents continually updated to the signature repository.
- Integration of research on threats specific to SLTTs, including nation-state attacks.
- CIS staff permanently deployed at the National Cybersecurity and Communications Integration Center (NCCIC) in Washington, D.C, thus facilitating valuable real-time information sharing with federal partners and critical infrastructure sectors.
- Availability of an Incident Response Team for forensic and malware analysis at no cost to SLTT government entities.
- Statistical analysis of traffic patterns to areas of the world known for being major cyber threats.
- Experienced cyber security analysts who review each cyber security event, which results in minimizing the number of false-positive notifications, allowing the first responder to focus on actionable events.
- 24x7x365 technical, research, and remediation support for cyber security incidents.

For these reasons **Vincent Hoang, Chief Information Security Officer, State of Hawaii - Office of Enterprise Services**, recommended that the Board of Water Supply should utilize this service stating; "*...the solution is uniquely provided by an organization designated by the Department of Homeland Security for the offering...*" Additionally, the State uses CIS **Albert** as their monitoring service.

BWS, being a local municipal utility identified as Critical Infrastructure by DHS, requires an ongoing, near real-time cyber security monitoring and incident response service tailored to and for government (SLTT)/Critical Infrastructure to ensure the resiliency of its operations. Without this service, we are at increased risk of cyber intrusion, resulting in operational impacts ranging from loss of customer information to water system compromises that threaten health and safety.

Other possible sources for the goods that were investigated but do not meet the BWS's needs

None – no other cybersecurity network monitoring service has the coordination with MS-ISAC, participation with NCCIC, designation of the Department of Homeland Security, and tailored for the SLTT and Critical Infrastructure sectors.

I certify that the information provided above is to the best of my knowledge, true, correct and that the goods described above are available through only one (1) source.


Kenrick Wong, Requestor


Henderson Nuuhiwa, Division Head

2/26/2019
Date

2/26/2019
Date

Direct Questions to: Henderson Nuuhiwa Phone: (808) 748-5275


Posting dates pursuant to Hawaii Administrative Rules Section 3-122-82:
MAR 29 2019 to APR - 5 2019

REVIEWED AS TO PROCUREMENT FORM:


VICKI KITAJIMA
Procurement & Specifications Specialist VI


4/5/19
Date

CERTIFIED AS TO AVAILABILITY OF FUNDS: 2019- 820 - 3021


FINANCE 8/3/19

3-29-19
Date

APPROVED AS RECOMMENDED/ NOT APPROVED


ERNEST Y. W. LAU, P.E.
Manager and Chief Engineer

4/5/19
Date

**BOARD OF WATER SUPPLY
CITY AND COUNTY OF HONOLULU**

March 29, 2019
(Date Notice Posted)

NOTICE OF INTENT TO ISSUE A SOLE SOURCE AWARD

The Manager and Chief Engineer is reviewing a request to make a sole source award to Center for Internet Security, Inc. to provide Netflow/Intrusion Detection System Monitoring and Multi-State Information Sharing and Analysis Service, known as Albert.

The award shall be made to:

Name of Vendor: **CENTER FOR INTERNET SECURITY, INC.**

Address of Vendor: 31 Tech Valley Drive
East Greenbush, NY 12061-4134

Amount of the contract: \$21,486.90

Direct any inquiries to: Robert Morita

Address: Board of Water Supply
Procurement Office
630 South Beretania St.
Honolulu, HI 96843

Telephone No.: (808) 748-5071

Fax Telephone No.: (808) 550-9193

Submit written objection(s) to this Notice of Intent to Issue a Sole Source Award contract within seven (7) calendar days from the date this notice was posted to:

Manager and Chief Engineer
Board of Water Supply
630 S. Beretania St., Room 201
Honolulu, HI 96843

Telephone No. (808) 748-5071

Sole Source Reference No.: BWS 19-08-SS

The Center for Internet Security (CIS) is a nonprofit organization focused on enhancing the cyber security readiness and response of public and private sector entities. CIS operates the Multi-State Information Sharing and Analysis Center (MS-ISAC), which is designated by the U.S. Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial (SLTT) government entities. Through its state-of-the-art 24/7/365 cyber security operations center, CIS serves as a central resource for situational awareness and incident response for SLTT governments, and offers a number of strategic cyber security services to assist in detecting, protecting, responding to and recovering from cyber threats.

The CIS Netflow/Intrusion Detection System Monitoring and Analysis Service, known as Albert, provides our partners with a near real-time automated process that identifies and alerts on traditional and advanced threats on a network, facilitating rapid response to threats and attacks. The Albert sensor(s) provide traditional Intrusion Detection System (IDS) monitoring, along with netflow and passive DNS collection and analysis. Through its 24/7/365 Security Operations Center (SOC), CIS manages the sensor(s) to identify malicious activity, and, in accordance with escalation procedures prescribed by the partner, provides notification of malicious activity. The use of open source software allows CIS to provide enhanced monitoring capabilities in a more affordable, cost-effective way than a typical commercial IDS/IPS solution. The Albert Service is available only from CIS.

Why is the CIS Albert Service Unique?

- Government-specific focus and tailored to SLTT government's cyber security needs.
- Correlation of data from multiple public and private partners
 - Historical log analysis performed on all logs collected for specific threats reported by partners and/or trusted third parties.
 - When a major new threat is identified, CIS will search logs for prior activity. (Traditional monitoring services only alert going forward, from the date a signature is in place. There is no "look behind" to assess what activity may have already occurred.)
- Statistical analysis of traffic patterns to areas of the world known for being major cyber threats. If abnormal traffic patterns are detected, analysts review the traffic to determine the cause, looking for malicious traffic that is not detected by signatures.
- Signatures from forensic analysis of hundreds of SLTT cyber incidents are added to the signature repository.
- Integration of research on threats specific to SLTTs, including nation-state attacks.
- CIS staff permanently deployed at the National Cybersecurity and Communications Integration Center (NCCIC) in Washington, D.C, thus facilitating valuable real-time information sharing with federal partners and critical infrastructure sectors.
- Experienced cyber security analysts who review each cyber security event, which results in minimizing the number of false-positive notifications, allowing the first responder to focus on actionable events.
- Availability of an Incident Response Team for forensic and malware analysis which is of no cost to SLTT government entities.
- 24/7/365 technical, research, and remediation support for cyber security incidents.



QUOTE

31 Tech Valley Drive
 East Greenbush, NY 12061
 www.cisecurity.org
 Federal Tax ID #52-2278213

Account Name	Honolulu Board of Water Supply, HI	Date Sent	3/13/2019
Bill To	Rm 6, 630 S. Beretania Street Honolulu, Hawaii 96834 United States	CIS Number	2018 PP Honolulu Board of Water Supply, HI-QTE-0006852
Contact Name	Henderson Niuhiviwa		

Quantity	Product	Sales Price	Total Price (USD)
12.00	NETWORK MONITORING & ANALYSIS SERVICE - UTILIZATION OF INTERNET CONNECTION - SIZE > 100 Mbps - 1 Gbps	\$940.00	\$11,280.00
12.00	NETWORK MONITORING & ANALYSIS SERVICE - UTILIZATION OF INTERNET CONNECTION - SIZE UP TO 100 Mbps	\$620.00	\$7,440.00
2.00	NETWORK SECURITY MONITORING & ANALYSIS SERVICE - SENSOR INITIATION SERVICE ONE-TIME FEE	\$900.00	\$1,800.00
	Tax		\$966.90
	Grand Total		\$21,486.90

Prepared By	Dawn Harnish	Phone	(518) 830-0766
Email	dawn.harnish@cisecurity.org		

Please refer any questions regarding this quote to Accounts Receivable at 518-266-3460 or email accountsreceivable@cisecurity.org

Please make checks payable to Center for Internet Security 31 Tech Valley Drive, East Greenbush, NY 12061