QUESTIONS AND ANSWERS FOR
REQUEST FOR PROPOSAL FOR CYBER SECURITY AUTOMATED THREAT EXCHANGE SYSTEM (ATIX)
Proposal Number 2014-1297

1) Are 6 references required (business and patient/ client) references? Is the second reference requirement for hospitals/ clinics?
   a. Patient/Client references are not applicable to this RFP. Submissions require only three business references from other customers who have received similar products or services.
2) Can you provide some detail Use Case examples of the User Account and what experience, Services or interactions they will expect to have with the MSSP, with the Fusion Center and ATIX?
   a. Cyber Analyst logs in, searches by a combination of temporal, geospatial, source, and malware parameters to view, for example, all observed SQL-injection attempts in August 2014 on Law Enforcement partners.
   b. Cyber Analyst is notified by email that malicious traffic has been observed to a known C&C server, gains additional information regarding common injection methods, observed symptom activity, and remediation steps.
3) Can you provide some detail Use Case of how you want to Compartmentalize and how to share the Regional Data and what types of Data you want your Users/Partners to have access to? How do you want to define your Partner/user or/and Fusion Center Roles? Defined by physical location only or by functional groups or does it matter?
   a. As it relates to Fusion Center coverage, the state of California is partitioned into five regions. Every partner that is a source of inbound data shall have the choice of sharing with all California Fusion Center Cyber Analysts, or with only the center within their geographic region. Outside of Fusion Center Cyber Analysts, users from partner sites only have visibility into their own data; one partner may not access data from another.

Entity	Who Can View Shared Information
Data Sharing Partner Example: local police department, hospital, university, etc.	- Approved staff from the partner organization - Cyber Security Analysts from regional Fusion Center - With partner permission, Cyber Security Analysts from other California Fusion Centers - Users from other partners *cannot* view

    b. For example:
        i. A hospital in San Francisco becomes a partner and wishes to share its data with all California Fusion Centers. That data is visible by Cyber Analysts from all California Fusion Centers, as well as applicable security staff from the hospital itself.
        ii. A university in Los Angeles becomes a partner, but only wishes to share with the Los Angeles Fusion Center. Cyber Analysts from the Los Angeles Fusion Center can see the data, as well as applicable security staff from the university, but it is invisible to Cyber Analysts from other Fusion Centers.
        iii. In all situations, to protect data privacy, users from partner sites have no access to other partners' data. Using the above examples, users from the hospital have no visibility into the status or activities of the university, and vice versa.

4) SECTION IV – SCOPE OF WORK, Item (4) asks that the 'solution' be capable of outputting to multiple formats. Can you expand on the use cases around this section so we're able to respond appropriately?
    a. At a minimum, CSV and PDF reports on observed malicious activity, malicious IP addresses, compromised systems and remediation guidance, etc. Machine-readable formats, such as STIX, TAXII, or YARA is a plus.

5) Do you want your new MSSP to provide the Security Monitoring services, correlation, detection and notification to the Client and the Fusion center? And if so how much do you want to be involved with the analysis, detection and response to your client?
    a. Yes – the proposed solution shall provide all monitoring, correlation, detection, and notification services. Partner users shall additionally have the ability to search their own submitted data, with Fusion Center users having visibility into all partners within their region, and statewide from partners choosing to share broadly.

6) Do we know how many potential entities and how many Devices for each we might be monitoring?
    a. 10-25 partner sites or data sources (firewall, IDS/IPS, SIEM, etc) should be covered by the proposal, with scalability costs to expand based on additional partners, events, or other metrics. Solution design should permit for unlimited growth.

7) Section 1 of page 11 (Platform Agnostic Data Collection) states the desire for a "zero-footprint connection (i.e. without installing proprietary software or hardware)" Does that mean we couldn't/wouldn't put a CTA (Collector) onsite at each of the partner's locations?
    a. This requirement is flexible; proposals may include options for a data sharing partner to engage via zero-footprint (e.g. syslog streaming), software collector, or hardware appliance integrations – with each providing varying levels of service or capabilities.

8) Firm qualifications and experience, including capability and experience of key personnel and experience with other public or private agencies to provide these services. This evaluation factor is the only place where 'key' personnel are mentioned. Are there specific job categories for the key personnel, or is it up to the offeror to determine which job titles will be key personnel?
    a. In this context, 'key personnel' are those staff members which would have a significant role in the development, deployment, and ultimate success of the proposed solution.

9) Compartmentalization of Sources and User Access: The solution must have the ability to compartmentalize data by California Fusion Center region (five regions total) and restrict access as desired by partner. Please identify/define the California Fusion Center “five regions total.”
    a. Northern California, Central California, Los Angeles, San Diego, and Orange County
10) Length of Agreement: The anticipated duration of the agreement will be for three years. Is the length of agreement intended to be inclusive of the solution development and ongoing monitoring or for three years of monitoring after implementation of the solution?
    a. Yes – three years “all inclusive” pricing is desired, though shorter durations may be agreed upon during contracting based on cost.
11) Please confirm if a version of the ATIX system currently exists or if the system is to be built by the proposer. If the system currently exists, would the county please provide access or specifications?
    a. The NCRIC currently does not provide nor utilize any managed services, distributed log correlation, or security appliance distribution.
12) Platform agnostic data collection. Can the county please provide a network diagram of the pre-existing Cisco, Checkpoint, Barracuda, Sonicwall, Palo Alto, or other major vendor network devices acting as firewalls, IDS, or IPS capacity within the NCRIC?
    a. We do not have this information. The list of - Cisco, Checkpoint, Barracuda, Sonicwall, Palo Alto – was meant to convey desired compatibility with common commercial firewall platforms that data sharing partners will have in place.
13) Where would the NCRIC like to have the consolidated data reside - Public Cloud, Private Cloud, Classified and/or on premise installation?
    a. Commercial or private cloud, preferably with CJIS or other Government data handling approvals.
14) In the section on Threat Intelligence it says, "Solution must compare collected data in real-time....”. Please define in more detail what "collected data” is referring to and provide any potential sources for comparison?
    a. Whatever data is necessary for the proposed solution to identify network security events in near real time. Potential examples are streaming syslog data from a Cisco firewall at the network’s perimeter, or listening to a SPAN port a Cisco Catalyst where data ingress/egress occurs.
15) Do they currently have a SIEM in place and if so what is it? Do they currently have a log management solution in place, if so what is it? Makes, models and quantities of security devices?
    a. The NCRIC chooses not to publically disclose its Information Technology security infrastructure. For the purpose of this RFP, assume the proposal will be protecting networks that only employ a perimeter firewall; no pre-existing SIEM, IDS/IPS, or log management to integrate with, and if those items are required for the overall solution, they should be included as new items in the proposal.
16) Any compliance requirements (FISMA, HIPPA, etc.)?

    a. The NCRIC does not impose any additional information security requirements upon data sharing partners, but content and method of data exchange would need to comply with any requirements of the partner.

17) Number of events they will be ingesting on a daily basis?
    a. Unknown, but assume typical business internet traffic for entities with approximately 100 endpoints or 10 Mbps bandwidth per site.
18) Requirements for IPv6 support?
    a. Not required
19) Is Management of the end point devices required?
    a. No management of existing workstations, servers, or security appliances is required. However, installation and configuration support is expected for new security appliances, data collectors, or any other components of the proposed solution.
20) Network connectivity?
    a. The NCRIC uses a 100 Mbps fiber-optic internet connection.
21) Dedicated or shared infrastructure?
    a. Data sharing partners will each present unique network infrastructure; the NCRIC has no information technology management authority over any partner.
22) Does the fusion center have to be in San Mateo County? Does it have to be in California?
    a. The NCRIC offices are in San Francisco, California. The location for collected data should reside in private or commercial cloud storage.
23) How many TOTAL locations need to be supported?
    a. An initial buildout of 10-25 sites should be covered by the proposal, with scalability metrics for unlimited expansion.
24) Do we need to register online to be considered?
    a. No, please submit your proposal via electronic and hardcopy as directed.