State of Delaware
Department of Technology and Information
QUESTIONS AND ANSWERS
DTI190032-MNGD_DETECT
Managed Detection and Response Provider
May 30, 2019

3	Question	Answer
1	**We'd be interested in the RFP but it asks for 3 years of audited financials. Most small firms with this expertise would have compiled or revB8:V12iewed statements. Would that work?**	RFP requires a vendor with strong state and local government managed detection and response experience. Proposals will be scored accordingly.
2	The due date specified of Thursday, May 30th 2019 conflicts with the Memorial Day holiday week. As a vendor which exclusively serves the US Public Sector market and whose employee mix contains a high percentage of veterans, Memorial Day is one of our most significant holidays. Many of our pursuit team members have long scheduled vacation time planned around the Memorial Day holiday to spend time with their families and remember the sacrifices of those who have served our country. **Accordingly, we respectfully ask for a three (3) week extension to accommodate those who have scheduled vacations bracketing both sides of the Memorial Day holiday week to support the ability to staff our solution team so that we may provide a high quality response to the State of Delaware.**	Please review the RFP and Addenda found here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N for the Procurement Schedule and submission due dates.
3	Section 5 Description of Firm Capabilities, Paragraph F - x, Page 8 "What is the process for adding additional log sources to the scope of service? Include the implications for deployment architecture, integration costs and ongoing costs." **Please describe the deployment architecture.**	Logs are forwarded through syslog or retrieved directly by our central log management and SEIM solution. Existing logs are centralized at this time.
4	Section 5 Description of Firm Capabilities, Paragraph C - v, vii, Page 5, "What percentage of your staff has security certifications (list the certifications), and what is the average number of years of experience they have in performing security monitoring or security consulting? Are there any differences based on geographic location and/or SOC in terms of your staff's certifications and experience?" **How many people do you currently have today performing security monitoring?**	DTI declines to answer. This information is not critical to be provided in order for Firms to draft a proposal.
5	Section 5 Description of Firm Capabilities, Paragraph E - ii, Page 7, "Explain your process for updating software to include signature updates and system patches. How do you ensure that this is done in a nonintrusive manner to your customers?" **Describe the maturity of the installation. (Has it been tuned and have patches and updates been maintained?)**	Current tools have been in place five years and are current in OS and Application patches and updates.

3	Question	Answer
6	Section 5 Description of Firm Capabilities, Paragraph A-x, Page 4, "Describe the typical workflow and process that occurs when the security analytics detects a security event, beginning with how that is presented to a SOC analyst for evaluation through the triage, validation, prioritization and customer alerting/notification process. Indicate where activities are automated versus manually performed by analysts." **What are the number of daily log events and how many security "events" are deemed interesting or require investigation on a weekly or monthly basis?**	This specific information can not be publicly shared. We write between 1.5 to 2 TB worth of logs from all security, systems and applications within the state.
7	Section 5 Description of Firm Capabilities, Paragraph A-vi, Page 4, "Explain support for the creation and management of customized correlation rules and the capabilities available to our staff for doing so. Describe any limitations, such as data sources, age and query frequency." **How many custom rules are currently deployed on the SIEM solution?**	This specific information can not be publicly shared. This question applies to vendors that require logs to be forwarded to their own SEIM solution. The question is intended to determine if the service provides the means for us to create customized rules and reports from your solution. This is access we currently have in our SEIM
8	Section 5 Description of Firm Capabilities, Paragraph I-x, Page 9, "Describe any integration capabilities with third-party service desk and ticketing tools and services. How is this achieved (e.g., email, application programming interfaces [APIs], etc.)? Also, indicate if you provide single-direction or bidirectional support, and whether the integrations are subject to additional costs." **What ticketing system is in use today to track incident response and security event and incident tracking ?**	ServiceNow
9	Section 5 Description of Firm Capabilities, Paragraph I-v, Page 9, "How does the portal provide us access to external threat intelligence feeds, in addition to the Department's own threat intelligence feeds?" **Does the state incorporate external threat intelligence feeds today? If so, which ones?**	Yes; the state uses multiple threat feeds. The question was to determine the threat intelligence the responders use.
10	Section 5 Description of Firm Capabilities, Paragraph G-u, Page 8, "Describe any specific network monitoring and/or network forensics features, capabilities or offerings to detect advanced, targeted attacks." **Please describe your incident response and digital forensics capabilities, staffing, tools, skills.**	This information is not available to responders. This is information we are asking for you to provide.
11	Section 5 Description of Firm Capabilities, Paragraph G-xii, Page 8, "How are big data platforms used to support the collection/analysis of network and endpoint data? Does your company require the deployment of its own network data collection/analysis solution? Can your company use the Department 's EDR solution, or is it mandatory that the Department use your company's EDR solution?" **What if any EDR do you current own and use?**	Crowdstrike

3	Question	Answer
12	Page 1 "Submission Due Date/Time: Thursday, May 30th 2019 at 2:00 P.M. Local Time" **Please let us know if we can get an extension for proposal submission by 2 weeks (by 13th June)**	Please review the RFP and Addenda found here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N for the Procurement Schedule and submission due dates.
13	Section 5 Description of Firm Capabilities, Paragraph A-ii, Page 3, "Indicate the ability to integrate with the Department's existing Security incident and event management system. Currently, the Department utilizes Splunk log management and SEIM." **Is the state flexible to move to a leveraged solution. What's the license expiry date for Splunk?**	Splunk license is perpetual.
14	Section 5 Description of Firm Capabilities, Paragraph A-ii, Page 3, "Indicate the ability to integrate with the Department's existing Security incident and event management system. Currently, the Department utilizes Splunk log management and SEIM." **Please describe Splunk license that you hold and if there is any need to procure or extend within the three year term.**	Licenses will be scaled out when the need arises and funding is available.
15	Section 5 Description of Firm Capabilities, Paragraph A-ii, Page 3, "Indicate the ability to integrate with the Department's existing Security incident and event management system. Currently, the Department utilizes Splunk log management and SEIM." **Please describe current log retention policy.**	12 months for most log sources; 7 years for systems in scope for compliance.
16	Section 5 Description of Firm Capabilities, Paragraph A-I, Page 3, **Describe whether the solution is Hardware or Software based.**	This question is to inquire if the solutions you leverage to deliver the managed service is software, virtual and hardware based. The state currently runs Splunk software on dedicated hardware.
17	Page 1, Project Description, **Elaborate on the type of devices reporting to SIEM (with count of each)**	3000 Nodes comprised of Firewalls, IPS, Proxies, Servers (Linux, Windows), VPN, Active Directory, Domain Controllers and various application logs.
18	Section 5 Description of Firm Capabilities, Paragraph G-xii, Page 8, **Do you currently use (own) any ATP solution**	Yes
19	**Describe restrictions on delivery location.**	If logs are to be shipped, must be US based and data cannot leave the US.
20	**Describe mandatory compliance requirements on the services offered.**	IRS1075, HIPAA, CJIS, PCI and other Federal, State and industry compliances.

3	Question	Answer
21	**If possible, list of security incidents in last few months. Else count with priority classification.**	This information is not available to responders during the bid process.
22	Section 5 Description of Firm Capabilities, Paragraph C-Qualifications and Staffing, Page 5, **Will DTI accept references from public sector entities outside of the US?**	Yes
23	Section 6 Staff Qualifications, Paragraph C-Example Projects, Page 12, **For "Example Projects" can we provide examples from non-US Public Sector entities ?**	Yes
24	Section number: 5.A Security Event Monitoring • Paragraph number:(i) • Page number: 3 • Text of passage being questioned: **What are the current target environment end-point, perimeter, network, and SOC security tools and mechanisms? For example: McAfee endpoint protection on servers and user devices, IDS/IPS, firewalls, load balancers on the networks, etc.**	The state has solutions in all the types mentioned here currently logging to our central log management and SEIM solution.
25	Section number: Project Information • Paragraph number: 1 • Page number: 1 • Text of passage being questioned: "… provide a Managed Detection and Response Provider (MDR) to augment its internal security teams with 24x7, 365 days …". **Are you seeking to augment your team with personnel from a contractor, have the contractor assume full operational responsibility and control of your SOC, team and tools, or some other arrangement?**	This is a managed detection and response service. Its not a request for individual contractors to augment our team. We are looking for specialized organizations that can integrate expert analytics, AI, industry proving use cases and expert security analyst experience into our logs to help identify actionable threats to the state and minimize the false positive noise.
26	Section number: Project Information • Paragraph number: 1 • Page number: 1 • Text of passage being questioned: "… provide a Managed Detection and Response Provider (MDR) to augment its internal security teams with 24x7, 365 days …". **What will be the role of the MDR vendor in regards to establishing security architecture and controls?**	The vendor may make recommendations for additional log sources, enhanced architectures to provide more visibility or enhancements to our internal SEIM for more actionable alerts and reporting.

3	Question	Answer
27	Section number: Project Information • Paragraph number: 1 • Page number: 1 • Text of passage being questioned: "… provide a Managed Detection and Response Provider (MDR) to augment its internal security teams with 24x7, 365 days …". **What is the "as-is" architecture and operational capability of your SOC? Please include how threat intelligence is obtained, and how incident response and forensics are undertaken.**	Logs are centrally collected, SEIM module within Splunk is configure to generate correlated alerts, this is coupled with alerts from our endpoint security vendor, managed service with MS-ISAC and multiple threat feeds into Splunk. The SOC is managed by Security analysts during the day and alerts managed by network operations center resources after hours. This RFP is for the managed detection and response company to provide 24x7 SOC services.
28	Section number: Project Information • Paragraph number: 1 • Page number: 1 • Text of passage being questioned: "… provide a Managed Detection and Response Provider (MDR) to augment its internal security teams with 24x7, 365 days …". **What is the target environment's characteristics in terms of devices, nodes, locations, etc.? Target environment is what the SOC will monitor.**	Logs are centrally collected, SEIM module within Splunk in one data center and backed up in another data center within the state.
29	Section number: Project Information • Paragraph number: 1 • Page number: 1 • Text of passage being questioned: "… provide a Managed Detection and Response Provider (MDR) to augment its internal security teams with 24x7, 365 days …" **Please provide an inventory of the security tools currently in use, and if those tools are leverageable by the MDR vendor.**	The state is looking for a vendor that can leverage any security solution at the states disposal. This can be a current solution or a future solution.
30	Section number: Project Information • Paragraph number: 1 • Page number: 1 • Text of passage being questioned: "… provide a Managed Detection and Response Provider (MDR) to augment its internal security teams with 24x7, 365 days …" **Are you seeking to have the contractor provide remedial actions on the target environment to include response to alerts including updating/patching the systems, managing hardware and software currency, and architecture configuration modifications and engineering?**	No, but we will evaluate and include in our decision making, vendors with other managed security services like firewall (UTM), IPS, Vulnerability management experience.

3	Question	Answer
31	Section number: Project Information • Paragraph number: 1 • Page number: 1 • Text of passage being questioned: "… provide a Managed Detection and Response Provider (MDR) to augment its internal security teams with 24x7, 365 days …" **Is there an ITSM solution such as Remedy, or ServiceNow in use to manage and track remedial actions initiated from the SOC?**	The state is a ServiceNow customer
32	Section number: Procurement Schedule • Paragraph number: Table • Page number: 2 • Text of passage being questioned: **What is the estimated award date?**	DTI is not able to share this information at this time.
33	Section number: Project Information • Paragraph number: NA • Page number: NA • Text of passage being questioned: **Is there an incumbent providing these services?**	These services are currently completed by internal resources
34	Section number: Network • Paragraph number • Page number • Text of passage being questioned: **How current is the environment today? N or N-1, How standardized is the environment.**	The environment is current
35	Section number: Network • Paragraph number • Page number • Text of passage being questioned: **What are the current volumes for each item: physical, virtual for network.**	That specific information is not available to responders at this time.
36	Section number: Network • Paragraph number • Page number • Text of passage being questioned: **What is the current network topology? 3-tier, flat, leaf?**	Multi-tier

3	Question	Answer
37	Section number: Network • Paragraph number • Page number • Text of passage being questioned: **Any wireless equipment in the environment?**	Yes
38	Section number: Network • Paragraph number • Page number • Text of passage being questioned: **What type of network monitoring is currently being used?**	SolarWinds
39	Section number: Network • Paragraph number • Page number • Text of passage being questioned: **What other network tools are in the environment?**	Infoblox
40	Section number: Incident Response • Paragraph number: H ii • Page number: 8 • Text of passage being questioned: **Is there a requirement or minimum of on-call support (1 or 2 people for Network/DCO)?**	The state has 24x7 network operations resources available and multi-tier on-call resources. The state expects 24x7, 365 around the clock monitoring and at least 2 hour responds to technical issues involving the vendor.
41	Section number: Incident Response • Paragraph number: H ii • Page number: 8 • Text of passage being questioned: **Is there a minimum requirement to how many tier 3 personnel need to be on a shift?**	No
42	Section number: Incident Response • Paragraph number: H ii • Page number: 8 • Text of passage being questioned: **What are the escalation procedures for tier 1/2/3 handoff?**	None

3	Question	Answer
43	Section number: Incident Response • Paragraph number: H ii • Page number: 8 • Text of passage being questioned: **What type of shift schedule is currently being used and how is that working for them?**	8 hour shifts
44	Section number: Staff Qualifications • Paragraph number: 1 • Page number: 12 • Text of passage being questioned: **How many network admins are supporting the current infrastructure?**	This information is not available to responders at this time.
45	Section number: I. Portals, Reports and Dashboards • Paragraph number: I. x. • Page number: 9 • Text of passage being questioned: **How interested is your organization to use SDN now or in the future?**	Not at this time.
46	Section number: 6 • Paragraph number: C • Page number: 11 • Text of passage being questioned "6. C. Example Projects: Example Projects provided are limited to ten (10) projects. Single-sided page for each project only. Public Agencies or Government examples are preferred." **Are the example projects included in the max 60 pages?**	Yes.
47	Section number: 6 • Paragraph number: B • Page number: 11 • Text of passage being questioned: "B. Resumes of Key Personnel Proposed for this Contract; Resume information is limited to eight (8) individuals regardless of affiliation. Each resume is limited to a single sided page." **Are the KP resumes included in the max 60 pages?**	Yes.

3	Question	Answer
48	Section number: 5.E Security Event Monitoring • Paragraph number:(iii) • Page number: 7 • Text of passage being questioned: "For each management service, indicate your change management process and your willingness to modify to meet our requirements." **Is there a preference towards using an existing Department ITSM system for change management vs using the MDR providers ITSM system?**	No preference but an integration with the State's ServiceNow system for incident handoff will be important.
49	Section number: 5.E Security Event Monitoring • Paragraph number:(iii) • Page number: 7 • Text of passage being questioned: "For each management service, indicate your change management process and your willingness to modify to meet our requirements." **If department ITSM system, what tooling in in place for consumption or integration?**	ServiceNow has API's for integration
50	Section number: 5.E Security Event Monitoring • Paragraph number:(iii) • Page number: 7 • Text of passage being questioned: "For each management service, indicate your change management process and your willingness to modify to meet our requirements." **Change management is only mentioned in this security event monitoring section under "E", but in section "A" which also is labeled as security event monitoring there is no mention of change management only notification and escalation. Will change management, to resolve a security incident, be managed by the Department or the MDR provider?**	By the Department
51	Section number: 5.F Security Information Management • Paragraph number: (vii) • Page number: 7 • Text of passage being questioned: "Indicate your standard data retention policies and ability to modify them to meet our requirements." **Please provide the current Department Data Retention policies and standards.**	7 years for compliance based systems and 12 months for other systems.
52	Section number: 5.G Advanced Analytics and Capabilities • Paragraph number: (xii) • Page number: 8 • Text of passage being questioned: **How are big data platforms used to support the collection/analysis of network and endpoint data?**	Splunk is considered a big data platform but an MDR vendor with strong AI and machine learning analytics capability will be rated highly.

3	Question	Answer
53	Section number: 5.G Advanced Analytics and Capabilities • Paragraph number: (xii) • Page number: 8 • Text of passage being questioned: "Does your company require the deployment of its own network data collection/analysis solution? Can your company use the Department's EDR solution, or is it mandatory that the Department use your company's EDR solution?" **Please identify the current Department EDR solution.**	The Department has an enterprise Splunk system and Crowdstrike endpoint security with its associated EDR service
54	Section number: iv. Indemnification • Paragraph number: 5 Performance Bond • Page number: 26 • Text of passage being questioned: **Is the bond required one time, after the award, or for every task order awarded?**	One time after award.
55	Section number: Pricing Spreadsheet • Paragraph number: • Page number: Pricing Summary • Text of passage being questioned: "Professional Services (lines 4 & 5) request pricing to: 1.Price to manage Splunk infrastructure on premise; 15 ingest and search heads 2.Price for infrastructure support" **To accurately price this effort, we require:** **1. The complete Splunk implementation and application details including hardware inventories.** **2. The complete infrastructure support requirements, inventories and volumes.**	This information is not currently available to responders. The quote should be generated based on the state number of log sources; 3000 and volume of logs per day; up to 2 TB.
56	Section number: RFP Overview/Project Requirements • Paragraph number • Page number: 2 • Text of passage being questioned: "DTI desires to select a pure staff augmentation company whose primary function is aimed towards providing services as outlined in this RFP." **Does this preclude vendors who are more than a pure staff augmentation company that provides complete Cyber Security services?**	Please review the RFP Addenda found here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N for the revisions to Project Requirements.

3	Question	Answer
57	Section number: Pricing Spreadsheet • Paragraph number • Page number: Pricing Summary • Text of passage being questioned: How should pricing for all years be shown. **There is only one price to be shown and it's unclear if the price to be shown should be for year 1, 2,etc.?**	Year one is requested, but any ongoing discounts would help with the decision making.
58	Section number: OVERVIEW OF SELECTION PROCESS – IDIQ • Paragraph number • Page number: 13 • Text of passage being questioned: "This is an indefinite delivery/ indefinite quantity agreement utilized for the performance of services on an as-needed basis. There is no guarantee of actual agreement value." **How will this IDIQ be utilized?**	On an as needed basis with Indefinite Delivery and Indefinite Quantity.
59	Section number: OVERVIEW OF SELECTION PROCESS – IDIQ • Paragraph number • Page number: 13 • Text of passage being questioned: "This is an indefinite delivery/ indefinite quantity agreement utilized for the performance of services on an as-needed basis. There is no guarantee of actual agreement value." **Will there be multiple vendors awarded the IDIQ?**	Please see the header of page 1 and page 18 Item O.
60	Section number: OVERVIEW OF SELECTION PROCESS – IDIQ • Paragraph number • Page number: 13 • Text of passage being questioned: "This is an indefinite delivery/ indefinite quantity agreement utilized for the performance of services on an as-needed basis. There is no guarantee of actual agreement value." **Will all awarded vendors receive future task orders to bid on the work or will only the top vendor based on scoring receive future task orders to bid?**	DTI is not able to share this information at this time.

3	Question	Answer
61	Section number: OVERVIEW OF SELECTION PROCESS – IDIQ • Paragraph number • Page number: 13 • Text of passage being questioned: “Selection Committee members will individually score each firm’s submitted proposal which determines individual ranking. The Department’s ranking is the combined ranking of all Committee members. Awarded firms, in order of ranking, will have the opportunity to negotiate an agreement with the Department. If the Department cannot reach agreement with the highest ranked firm(s), the Department terminates negotiations and begins negotiations with the next highest ranked firm, and so on until an agreement is reached. The Department notifies via email the awarded firm(s) of the opportunity to enter into an agreement with the Department. This notification also includes information on the next steps for the agreement process. “ **This paragraph implies that only one vendor will be awarded the IDIQ. Is that correct that only one vendor will be awarded this IDIQ?**	Please see the header of page 1 and page 18 Item O.
62	Section number: 5 •Paragraph number: F (i) •Page number: 7 •Text of passage being questioned: "Indicate the data sources supported for log collection, reporting and retention. Can logs be collected from any source? Describe the collection methods (e.g., forwarded syslog, Windows Management Instrumentation [WMI], local forwarding agent)." **Is the IBM z/OS® (Mainframe) being included as a required data source for monitoring in this RFP?**	The IBM Z/OS is already being logged into the departments SEIM solution and should be part of the monitoring agreement.
63	Section number: 5 •Paragraph number: A (i) •Page number: 3 •Text of passage being questioned: "Indicate the capabilities of your services to monitor our firewall, intrusion detection system (IDS), intrusion prevention system (IPS), domain controllers, applications, endpoint security tools, identity and access management, network/server device logs, URL filtering, vulnerability data and any other security related systems." **Can you provide an exact list of all platform that are a requirement for log monitoring on this RFP?**	This information can not be shared at this time.
64	Section number: 5 •Paragraph number: A (xi) •Page number: 4 •Text of passage being questioned: "Indicate the level of interaction and support that our staff can expect from your security analysts to assess, investigate and respond to incidents." **Is this RFP meant to be responded to by Managed Service Providers?**	Yes

3	Question	Answer
65	Section number: 5 • Paragraph number: A (ii) • Page number: 3 • Text of passage being questioned: "Indicate the ability to integrate with the Department's existing Security incident and event management system. Currently, the Department utilizes Splunk log management and SEIM." **Is the goal for the MDR contract winner to send the data collected from the organizations platforms on to Splunk, or is DIT going to be sending Splunk log data on to the MDR contract winner's environment for analyzing and response?**	DTI expects the vendor to either leverage the state's Splunk solution or forward the logs to its own SEIM solution for analysis.
66	Page 2 Procurement Schedule **Can we ask that the date of all questions due be moved to May 24th, 2019?**	Please review the RFP and Addenda found here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N for the Procurement Schedule and submission due dates.
67	Page 2 Procurement Schedule **Can we ask that the answers to all questions asked by vendors be provided to all vendors – 12 days prior to the due date of the RFP?**	The Procurement Schedule can be found in the RFP and Addenda here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N
68	Page 2 Procurement Schedule **Can we get an extension on the due date of the RFP response to June 20th, 2019?**	Please review the RFP and Addenda found here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N for the Procurement Schedule and submission due dates.
69	Page 2 – Project Requirements DTI makes a statement that the desire is that this solution be pure "Staff Augmentation". **Is a solution that uses off site personnel in a SOC acceptable?**	This service assumes the use of resources that are offsite. These resources must be in the continental US.

3	Question	Answer
70	Section: Procurement Schedule Paragraph Number 1, Page 2 Text: Final Response to Questions posted by Five (5) business days prior to the proposal due date, 2:00 P.M. Local Time: **Can the State provide a 2 week extension for the due date for the RFP response? The timeline posted only allows 5 business days prior (May 24th) to the RFP due date of May 30th to review the State's answer to questions. The answers to questions are a critical component of developing a solution that meet the technical requirements set forth in the RFP and limiting the time to 5 Business Days between Q&A "posting" and the due date will negatively impact ability to develop the best proposal**	Please review the RFP and Addenda found here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N for the Procurement Schedule and submission due dates.
71	Section: PROPOSAL REQUIREMENTS Paragraph Number 2, Page 3 Text: Submit one (1) original hard copy of the Proposal. Receipt of insufficient copies or non-compliance with providing the requested information in the desired format, may negatively impact the scoring. Proposals cannot exceed sixty (60) pages excluding Appendix A Required Forms and Appendix B Pricing Spreadsheet. **Can the State expand the limit of a 60 page response?** **Based on the RFP requirements, quantity and depth of the questions, including questions within questions, we are requesting a modification to the 60 page limit. This limit prohibits our ability to provide a comprehensive proposal that adequately addresses all the state's requirements and questions.**	Please review the RFP and Addenda found here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N for Proposal Requirements.
72	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment....." **Do you want the MDR to manage the existing Splunk environment, in addition to ingesting logs / reporting on malicious activity?**	No

3	Question	Answer
73	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment……" **Do you currently have any custom use cases developed within Splunk? Is your intent to leverage the MDR for assistance / guidance in creating Splunk use cases? (i.e.. a non-incident event that is of customer interest, such as a server connecting to another device)**	Yes; its our intent to leverage the MDR to assist with internal Splunk use cases where necessary.
74	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment……" **Please confirm your inventory of assets /devices you require monitoring / analytics for?**	This information cannot be shared at this time.

3	Question	Answer
75	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment....." **What is your current Splunk Enterprise License size (gig per day)?**	2 TB
76	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment....." **What is your current security-only log ingestion (gig per day)?**	We consider all logs collected to have security implications. About 1.2 TB are security related.

3	Question	Answer
77	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment……" **What is your current network / infrastructure log ingestion (gig per day)?**	.3 to .8 TB other logs
78	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment……" **How many actionable incidents do you triage on a monthly basis?**	This information is not available at this time.

3	Question	Answer
79	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment....." **Is this raw log data or compresses log data?**	This is raw log ingestion
80	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment....." **Of the 2tb of daily log ingest volume, how much of this is actionable security logging?**	1.2 TB

3	Question	Answer
81	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment....." **How many locations are currently serviced with your SIEM / security platform?**	All locations write to a single SIEM platform at our primary data center
82	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment....." **Do you have any specific regulatory requirements such as HIPPA, FERPA, PCI, ISO, etc.?**	IRS1075, HIPAA, CJIS, PCI and other Federal, State and industry compliances.

3	Question	Answer
83	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment……" **Is the MDR required to store customer logs, or only scan and drop logs for actionable security incidents?**	The MDR is required to store even customer logs to enable historic event analysis and trending.
84	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment……" **Are there any requirements that customer log data reside within the Continental US?**	Yes

3	Question	Answer
85	Section: Project Description Pages 1 and 2 Text: "The MDR will work as an extension of the Department's internal security team to monitor logs collected from an environment with up to 3000 nodes and 2TB daily log ingest volume. The MDR will be expected to leverage the Department's internal log management system alongside the MDR's own proprietary log correlation rules and analytics in the detection of actionable attacks against the State. The MDR must be able to understand the State computing environment, accurately assign risk levels to threats and monitor the environment in real-time, 24x7 with real-time threat response. The MDR may be required to tune and enhance the Department's SEIM solution in order to ensure its effectiveness in correlating threat events into a security incident. The MDR will work with the Department to establish a playbook with information on when and how to contact the internal security team to take steps to stop an attack. The MDR will be required to make the recommendations on the required log sources and event auditing requirements and logging levels to ensure they have the information necessary to effectively detect an attack, malware or a breach of the State's computing environment……" **Are there log retention requirements that the MDR must comply with?**	6 months worth of security actionable event logs
86	Section: Project Requirements Page 2 Text: "DTI desires to select a pure staff augmentation company whose primary function is aimed towards providing services as outlined in this RFP." **How does the state define "a pure staff augmentation company"?**	Please review the RFP Addenda found here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N for the revisions to Project Requirements.
87	Section: Project Requirements Page 2 Text: "DTI desires to select a pure staff augmentation company whose primary function is aimed towards providing services as outlined in this RFP." **Are you looking for staff augmentation services to supplement your staff for SIEM, Splunk use-case development, rules tuning, device management, Emergency Response, etc.?**	NO; the state is looking for a pure play managed detection and response services company in the managed security services space. The vendor may be leveraged for other security functions as required. These functions may be negotiated as part of the contract process.
88	Section: Project Requirements Page 2 Text: "DTI desires to select a pure staff augmentation company whose primary function is aimed towards providing services as outlined in this RFP." **Would the state consider a managed service provider (as opposed to a traditional staff augmentation), as long as this meets the technical requirements of this bid?**	Please review the RFP Addenda found here: http://bids.delaware.gov/bids_detail.asp?i=5711&DOT=N for the revisions to Project Requirements.

3	Question	Answer
89	Section: A. Security Event Monitoring Page 3 Item 5Ai Text: "Indicate the capabilities of your services to monitor our firewall, intrusion detection system (IDS), intrusion prevention system (IPS), domain controllers, applications, endpoint security tools, identity and access management, network/server device logs, URL filtering, vulnerability data and any other security related systems. " **Item 5.A.I - Would it be possible to get a breakdown / inventory of the 3000 nodes in regards to device type (i.e.. firewall, router, workstation, server, IPS, etc.)**	No
90	Section: A. Security Event Monitoring Page 4 Item 5A XI Item 5.A.XI – **What level of Incident Response is required from the MDR for this bid? Should the MDR include staffing / resources to perform incident response for this bid?**	The state will like to assess the quality of resources assigned to perform this service on behalf of the state for this contract.
91	Section: D. Implementation and Service Methodology Page 5, 6 and 7 Item 5.D.V **What infrastructure is being supported, and what level of support is requested from the MDR?**	The enrollment of the state into the service
92	Section: D. Implementation and Service Methodology Page 5, 6 and 7 Item 5.D.V **Do you want the MDR to provide device management, health availability, policy services for your existing premise based security devices? If yes, please confirm those devices.**	The MDR may be leveraged for firewall (FortiGate), SEIM(Splunk) or Tenable Vulnerability Scanning solutions outside the MDR agreement.
93	Section: Pricing Item: Pricing Worksheet **The pricing requests cost for providing infrastructure support.** **What infrastructure is being supported, and what level of support is requested?**	The MDR may be leveraged for firewall (FortiGate), SEIM(Splunk) or Tenable Vulnerability Scanning solutions outside the MDR agreement.
94	Revised Due date now June 6th- **Does the change in RFP due date, impact the timeline for other deliverables, specifically for the posting of the Q&A? Will the Q&A be posted to per the original time which would equate to May 24th or will that date be pushed back another week in alignment with the due date?**	The procurement schedule will adjust based on the date proposals are due.

3	Question	Answer
95	The State struck the term “staff augmentation” from the Project requirements DTI desires to select a pure managed detection and response staff augmentation (struck) company whose primary function is aimed towards providing services as outlined in this RFP. **Please define how the State interprets the term “staff augmentation”**	The state does not plan to identify a named resource to assist its team. The state is looking for an organization that can perform this function with what ever technology or number of resources required to effective accomplish the monitoring tasks assigned.
96	The State struck the term “staff augmentation” from the Project requirements DTI desires to select a pure managed detection and response staff augmentation (struck) company whose primary function is aimed towards providing services as outlined in this RFP. **Does the State no longer require a resource to be on site at DTI to support the existing DTI Security resources?**	No onsite resource required.
97	Page 6, section 5.D.vii **What ticketing system is currently in use, that the MDP vendor would interface with?**	Service Now
98	Page 6, section 5.D.viii **What Enterprise Directories & CMDB system are currently in use, that the MDP vendor would interface with?**	ServiceNow
99	Page 7, section 5.E.i through 5.E.v **Is the intent of this RFP for the MDP vendor to physically (onsite) and virtually (remotely) manage the client's security devices? If so, please provide a list of all security devices to be managed as part of this RFP. If devices are not running current code (i.e.. IOS, patches), is it the responsibility of the MDP provider to baseline all devices, and update them to current revisions of code?**	This is a remotely managed service
100	Page 7, section 5.E.i **What devices are considered "in scope"**	Firewalls, IPS, URL filtering, domain controllers, mainframe, web logs, reverse-proxy logs, application logs, Vulnerability Scan, etc.
101	Page 7, section 5.E.ii **Is the intent of this RFP for the MDP vendor to patch and update the client's security technologies? Or does this only relate to the MDP's infrastructure that is utilized to perform the MDP functions as outlined in this RFP?**	The MDR may be leveraged for firewall (FortiGate), SEIM(Splunk) or Tenable Vulnerability Scanning solutions outside the MDR agreement.

3	Question	Answer
102	Page 8, section 5.F.vii **Is there a requirement for 366 days of storage for collected logs?**	Storage of logs at the MDR is limited to 6 months
103	Page 8, section 5.G.xii **Is the intent of this RFP for the MDP vendor to provide a separate EDR solution?**	No
104	Page 8, section 5.G.xii **What is the company's current EDR solution?**	The State has Crowdstrike and MS-ISAC as current EDR services
105	Page 8, section 5.H.i **Is the intent for the MDP vendor to provide onsite and / or remote Incident Response as part of this RFP, with cost included in the pricing worksheet?**	Remote managed incident detection and response is what is expected.
106	Page 10, section 5.J.iv **What Service Level Agreements are requested to be "outlined in the scope" of this RFP? Are there any pre-defined penalties for violation of these RFPs?**	A 2hr detect and alert SLA for threats against the state.
107	Page 10, section 5.J.vii **Please provide a list of "in scope" devices and software for this RFP.**	The MDR may be leveraged for firewall (FortiGate), SEIM(Splunk) or Tenable Vulnerability Scanning solutions outside the MDR agreement.
108	Page 10, section 5.J.x **Could you provide an example of a change that would be considered in scope for this RFP?**	Adding a new log source to the monitored environment.
109	Page 26, section G.iv.9 **Could you provide an example of work being assigned in this question that would be considered in scope for this RFP?**	Adding a new log source to the monitored environment.
110	Page 26, section G.iv.30.e **Could you provide an example of status reports that would be provided in delivery of this RFP?**	Metrics on threats identified and false positive noise reduction

3	Question	Answer
111	Section A Paragraph 1 Page 4 "Indicate the capabilities of your services to monitor our firewall, intrusion detection system (IDS), intrusion prevention system (IPS), domain controllers, applications, endpoint security tools, identity and access management, network/server device logs, URL filtering, vulnerability data and any other security related systems. **Our Managed Detection and Response Service is a comprehensive approach that does not require any existing SIEM and can provide a significant costs savings to maintaining your own SIEM. That being said, if our service is a fit for your requirements, would you be open to the idea of removing your existing SIEM?**	We may be open to making our existing SEIM more of a log manager if the service is effective enough to establish that level of confidence.
112	Section A Paragraph 2 Page 4 "Indicate the ability to integrate with the Department's existing Security incident and event management system. Currently, the Department utilizes Splunk log management and SEIM." **Is your existing SIEM licensed on a perpetual model or an annual model?**	Yes, Perpetual.
113	Section K Paragraph 4 Page 11 "Provide the base cost and pricing methodology." **How many "knowledge workers" do you have, where a knowledge worker is a full time employee that leverages the network/information systems on a daily basis?**	5
114	Section K Paragraph 4 Page 11 "Provide the base cost and pricing methodology." Do you utilize Office365 or GSuite? If so, how many users are you licensed for?	The Department declines to answer as this information is not required in order to respond to this RFP.
115	Section K Paragraph 4 Page 11 "Provide the base cost and pricing methodology" **How many servers do you have in your environment, including both physical and virtual?**	We are not looking for per server pricing. We need log source and ingest per day pricing
116	Section K Paragraph 4 Page 11 "Provide the base cost and pricing methodology." **Do you utilize Azure or AWS for IaaS? If so, how many servers are you running, on average?**	Not at this time.

3	Question	Answer
117	Section K Paragraph 4 Page 11 "Provide the base cost and pricing methodology." **In your main network hub / datacenter, what is your internet connection type (1 G Fiber, 10 G Fiber, etc.) and what is the bandwidth capacity? What is the average utilization? (i.e.: 500 Mbps)**	10G
118	Section K Paragraph 4 Page 11 "Provide the base cost and pricing methodology." **Does your main network hub utilize Active/Active HA Firewalls?**	N/A we have capacity for 10GB throughput
119	Section K Paragraph 4 Page 11 "Provide the base cost and pricing methodology." **In your other locations, is the network setup so that all traffic is backhauled to your main network hub / datacenter?**	Yes
120	Section K Paragraph 4 Page 11 "Provide the base cost and pricing methodology." **If your traffic is not backhauled from your other locations, but instead has a direct route to the internet, please provide the internet connection details for each location. (Physical link type, bandwidth capacity, average bandwidth utilization, HA Firewalls or not, etc.)**	Traffic is backhauled
121	Section K Paragraph 4 Page 11 "Provide the base cost and pricing methodology." **Do you wish to have Continuous Vulnerability Assessment (iVA, eVA, hVA) included in our proposal?**	Continuous vulnerability assessment can be priced separately from the monitoring service.
122	Section F Paragraph 2 Page 7 "Will all our raw event logs and data be collected and forwarded to your platform for storage? If no, describe the variation and options for full log event retention (if applicable)." **Do you have a requirement to store raw log data for a particular amount of time?**	6 months worth of security actionable event logs
123	Section D Paragraph 5 Page 6 "Explain how these services, and any supporting products will use or interface with products the Department has in place will be affected by outsourcing, such as intrusion detection and vulnerability analysis. Ensure that you include details on how you intend to connect to the Department's infrastructure to provide support." **Please provide the names of the products you are currently using for security so that we can validate compatibility with our service. (IDS, IPS, Firewall, Endpoint/AV, etc.)**	The MDR may be leveraged for firewall (FortiGate), Crowdstrike, SEIM(Splunk) or Tenable Vulnerability Scanning solutions outside the MDR agreement.

3	Question	Answer
124	Section 5.A.ii., Page 4, "Indicate the ability to integrate with the Department's existing Security incident and event management system. Currently, the Department utilizes Splunk log management and SEIM" **Is DTI interested in a Co-Managed solution (i.e. both the customer and service provider have access to the Splunk SIEM platform 24/7)?**	That can be discussed if proposed.
125	Section 5.A.ii., Page 4, "Indicate the ability to integrate with the Department's existing Security incident and event management system. Currently, the Department utilizes Splunk log management and SEIM" **When referencing Splunk SIEM, please confirm that DTI utilizes Enterprise Security.**	Yes, we do
126	Section 5.A.ii., Page 4, "Indicate the ability to integrate with the Department's existing Security incident and event management system. Currently, the Department utilizes Splunk log management and SEIM" **Will DTI provide direct access to its current Splunk Enterprise Security environment so analysts can manage, monitor, hunt, and respond to threats?**	Yes
127	Section 5.A.ii., Page 4, "Indicate the ability to integrate with the Department's existing Security incident and event management system. Currently, the Department utilizes Splunk log management and SEIM" **Is DTI open to keeping all its log data in its current environment?**	Yes
128	Section 5.C.v., Page 5 "What percentage of your staff has security certifications (list the certifications), and what is the average number of years of experience they have in performing security monitoring or security consulting? Are there any differences based on geographic location and/or SOC in terms of your staff's certifications and experience?" **Are offshore SOC's acceptable or do all SOC's need to be US based, manned by US Citizens?**	US based SOC resources
129	Section 5.F.viii. "Is there a minimum and maximum of times that log retention can be offered? Describe what is actively available versus what is kept offline. If 366 days of storage is required, how will that be priced for the Department?" **Do security analysts assigned to the DTI account need to certified in Splunk and Splunk Enterprise Security?**	No

3	Question	Answer
130	Section 5.F.viii. “Is there a minimum and maximum of times that log retention can be offered? Describe what is actively available versus what is kept offline. If 366 days of storage is required, how will that be priced for the Department?” **Does DTI’s current Splunk infrastructure retain logs for the duration suggested (366 days)? If not, would the capability to expand the existing infrastructure to meet the requirements be possible?**	Yes
131	**Are there any compliance requirements to be met with this Managed SIEM solution? If so, please describe.**	7 years for compliance based systems and 12 months for other systems.
132	**Please describe any recurring operational/security pain points.**	Log source upgrades, moves or changes.