Questions and Answers for RFP #648689

1) On the Page 4 network diagram, please confirm that the IPS will be supporting a 1 Gig throughput as depicted in the diagram.

Confirmed.

2) Page 5, Overview: A good IRRFT also has the ability to do event correlation and analysis. What is the meaning of analysis in this context?

The IRRFT should have basic capabilities to present analysis reports of data collected by the sensor(s). Summary reports listing general statistics about events observed by the unit are an example of analysis in this context.

3) Page 6, 1c: By stateful protocol analysis, do you mean it must be able to identify application level protocols (i.e. protocols not necessarily running on a standard port)?

Stateful protocol analysis simply adds stateful characteristics to regular protocol analysis. Simple protocol analysis is limited to examining a single request or response. Stateful protocol analysis monitors all of the events within a connection or session.

4) Page 6, 1c, iv: What do you mean by TCP state verification?

This is the ability to determine if a TCP connection is in "active open" or "passive open", "half close" or "active close" state.

5) Page 6, 1d, ii: Which protocol violations must it detect? Which protocols must this be in affect against?

Please list the protocols your product is capable of detecting a violation. Example protocols are listed in Page 6, 1c, i.

6) Page 6, 2c: To further understand your question, can you be more specific or clarify the goal?

We would like to know if your product is capable of detecting individual fragments of exploit code. Signature analysis is the common method of doing this.

7) Page 7, 2b: Can you clarify the purpose of logging stateless connections and when you want this triggered?
Stateless connections are those in which no information about the connection is retained by the sender or receiver. There are attacks that use this mechanism.

8) On Page 9, point (h), the statement refers to distributing signature library and policy "on a per host basis". Does this refer to individual IPS/IDS systems (in a multiple IPS/IDS deployment)?

Yes. This does refer to individual IPS/IDS units in a multiple IPS/IDS deployment. If your proposal includes multiple IPS/IDS sensors, explain how the individual sensors are updated as well as the frequency of updates.

9) Will a vendor’s solution that does not support IPv6 today, but that will support it in the future via a software update, be eliminated from consideration of this award?

Most products researched today are capable of handling IPv6 traffic.

10. When is the deployment?

Deployment is ASAP. Sometime in the next 60 days if possible.

11. Ipv6: How strict is this requirement?

Your system should be able to pass Ipv6 traffic today.
Additional Question & Answer for RFP 648689

1. Must be able to detect IPv6 attacks. Does VA Tech want this today or on the roadmap for the future?

The product should be able to handle IPv6 traffic today.