The government recognizes the complexity of a full Zero Trust Architecture (ZTA). The government further recognizes no single vendor will address all aspects of a ZTA. When addressing the scenarios provided below, clearly state the following:

- Aspects of ZT (as previously defined by the government in association with the working group) that your solution addresses
- The specific protects your solution provides aligned to the scenario
- Identify any standing partnerships you have with other vendors for meeting other aspects of ZT
- Identify any operational deployments of your solution in either a government setting or private industry, providing specifics on the operational setting (size of agency, etc.)

Unless otherwise state, assume an unclassified (or SBU) setting.

Scenario 1
An agency employee is working remotely, using personally owned devices, must regularly access a public cloud based, agency application. The employee routinely accesses the system as a standard user but occasionally switches to administrator mode to perform systems maintenance. The user's physical location changes frequently with personal travel.

Scenario 2
An agency employee, working on from an agency satellite office and using government furnished equipment, is accessing Internet sites. The sites vary between sites supporting job related research and his/her personal bank. Limited personal use is acceptable per agency policy.

Scenario 3
A contracted employee provides ongoing improvements to an agency system as part of a development team and provides administrator and routine maintenance to the operational system. Development is performed from the contracted employee's corporate offices using devices provides by his/her company. Development is performed on a separate network, isolated from the production network. Both operate within a data center located at the agency's facilities. When appropriate, the contracted employee moves systems from the development environment into production.

Scenario 4
Use the conditions described in Scenario 3 but both the development and production systems are cloud-based.

Scenario 5
An agency system interfaces with another agency's system, accessing fingerprint information as part of a background investigation process. Both systems are public cloud-based.

Scenario 6
Use Scenario 5 but both systems are located on-premise in the agencies' data centers.

Scenario 7
Use Scenario 5 but the primary system is located on-premise in the agencies' data centers and the secondary, accessed system is in a public cloud.

Scenario 8

Use Scenario 5 but the primary system is housed in a public cloud and the secondary, accessed system is located on-premise in the agency's data center.

Scenario 9

Use Scenarios 5 through 8 above but address from the perspective the primary agency system is being accessed to gain fingerprint data by another agency's system.

Scenario 10

The remote users (e.g. telework, off-site) of an agency's cloud-based HVA system are having connectivity issues that are inconsistently kicking them off their session. Outline any tools you provide for administrators' troubleshooting.

Scenario 11

The ICAM administrator has reported a user's credentials were compromised. Describe any tools/methods you provide to validate unauthorized access to systems under the ZTA umbrella has not occurred, either on-premise or cloud-based.

Scenario 12

An agency has decided to perform penetration exercises against their HVA systems operating under the ZTA umbrella, both on-premise and cloud-based. Describe the tools/methods you provide or support to accommodate these penetration exercises.