**Internet Connectivity Divestment Detailed Questionnaire**

*\*Note: The below additional questions should copied and pasted into a new document as needed based on answers to the first questionnaire (“1-Internet Connectivity Divestment Initial Questionnaire”). These additional questions should be sent to the divestment project manager.*

**General DMZ**

1. Is network device redundancy needed in the DMZ and its associated services?
2. Is site DMZ redundancy needed for the divestment?
3. Will network hardware and licenses be purchased for the divestment or will it need to be sourced from existing inventory? If it will be sourced from existing inventory, then what devices are available?
4. If Cisco Firepower devices running FTD software are being used, has a virtual FMC been provided to manage them? If no, then a virtual FMC will need to be purchased.
5. Have the internet circuit(s) been ordered? If yes, then what is the circuit bandwidth(s) and the delivery date(s)?
6. How many sites will be divested? If there are multiple sites, will each site have their own internet and/or extranet link or will the traffic pass through centralized location(s)?

**Corporate VPN (CorpVPN)**

1. How many users will be using the CorpVPN service?
2. How many and which locations will need this service?

**Third Party Remote Access (TPRAS) VPN**

1. For clientless access using a browser, what is the Citrix homepage URL (i.e. Web Interface/StoreFront) to which users should be re-directed after successful login?
2. Who is the purchasing company contact who will be handling the creation of the external (i.e. DigiCert, Entrust, etc.) SSL certificate needed for the public-facing interface of the TPRAS VPN gateway?
3. How many and which locations will need this service?

**Third Party Site-to-Site (TPS2S) VPN**

1. How many site-to-site third party VPN connections will the divestment need to migrate?
2. What are the NECT numbers for each connection?
3. What is the technical contact information of either the third party customer or the business owner responsible for each of the connections?
4. How many and which locations will need this service?

**Extranet**

1. How many third parties with dedicated circuits will need to be migrated (include all services that may be shared with other business units or might be connected through a regional connection instead of a local one to the site)?
2. Is it possible to migrate the extranet customer(s) from a dedicated circuit to a site-to-site (S2S) VPN connection?
3. If the third party cannot migrate to S2S VPN, then has the new extranet dedicated circuits been ordered? (If yes, then when will they be delivered?)
4. Are there any external user interactive inbound traffic for the extranet connections? If yes, then will the authentication used for the external user be SecureAuth or RSA?
5. What are the NECT numbers for each connection?
6. Do we have the technical contact information of either the third party customer or the business owner responsible for each of the connections?
7. How many and which locations will need this service?

**F5 Services**

1. What are the host machines on which the virtual F5 BIG-IP images can be installed? If there are no host machines available, then will a physical appliance be purchased?
2. Who is the purchasing company contact who will be handling the creation of the external (i.e. DigiCert, Entrust, etc.) SSL certificate needed for the public-facing VIPs (Virtual IPs)?
3. How many and which locations will need this service?

**IBM Services**

1. If a dedicated connection is being used, then has the circuit been ordered (include bandwidth and delivery date)?

**DMZ On-Prem Applications**

1. What are the applications or services that need to be placed on-prem in the DMZ?
2. What are the inbound applications or services that need F5 load balancing?