Security Intake form for Netscaler/FLEXPod

- **SYSTEM IDENTIFICATION**
  - Date of Application
  - Name/Title of Application/System
  - Responsible Organization(s)
  - Full POC information, including 7X24 contact info. Please also list the preparer of this document, if different than the POC.
- **GENERAL PURPOSE/Description**
  - List all hosts that supply data for this Application
  - Show data flow of data from input(s) to output
  - Please give a description of what this application does for your department.
  - If possible, please show this in a drawing
- **SYSTEM ENVIRONMENT**
  - Please note ALL systems that supply data, their physical location and IP addressing.
  - For each host, include what TCP/IP ports are exposed to the internet and for what purpose.
  - If there exists a test systems, please document that here, and any ACLs they may have
  - Any interconnects or information sharing across agencies?
  - What sensitive data may flow from/thru this system? Please denote applicable regulations or laws that may govern data contained within, specifically dataloss related information.
  - USE OF Web Application Firewall. If using ETS supplied Netscaler/WAF, please skip
    - Please fully describe what application firewall is being used, who maintains it, and what it tests for.

- **MANAGEMENT CONTROLS**
  - What measures are in place to prevent unauthorized access
    - Are user accounts based on SOA Active Directory? If not, what account controls are in place.
    - Are there periodic reviews of user access by system or data owner? Please describe what reviews are done.
    - Where is the data access being logged, where and for how long?
    - Is console and file system access logged, where and for how long?
    - Is new content tested in a test environment before going live?

- **PRODUCTION/Input Output CONTROLS** (if using ETS hosted services, please skip)
  - Please list all platform(s) you are using for this service. Operating system/patch level, etc.

- Anti-Virus/Zero Day Tool Installed? If so, what product.
- What schedule do you patch the operating systems?
- What are the procedures for updating the application and application server? How often do that occur.
- Has this system been “hardened” and by what means?
- Is physical access limited to this host(s)? If so, how?
- Who has access to the local console(s)?
- Is there remote desktop access to this server, how is that controlled? Is there a restriction banner displayed upon remote login?
- What backups are in place, and what if any Disaster Recovery (DR) procedures are in place for this application.