Agriculture Security Operations Center

Please complete all applicable fields and return for closure consideration to cyber.incidents@asoc.usda.gov or contact the ASOC Hotline at (866) 905-6890.

Section I: Identification (if false positive, complete only this section)	
Employee Name/Title:	
Hostname/Username:	
IP Address:	
Domain:	
Operating system and version:	
CSAM system name:	
Is it a high value asset?	
Equipment Location (physical address):	
How was the incident discovered?	
If IP Addresses/URLs were blocked at the agency firewall, provide list with date/time implemented.	
Date/Time the computer was removed from the network:	Choose a Date/Time
Functional Impact: (None, Low, Medium, High)	Choose an item.
Informational Impact: (None, Integrity, Privacy, Proprietary, Classified)	Choose an item.
Recoverability: (Not Applicable, Not Recoverable, Extended, Supplemented, Regular)	Choose an item.
Server Information (if applicable)	
What functions does this server perform?	
System owner:	
Operating system and version:	
Antivirus software and version:	
Most recent patch update:	
Is the server accessible by internet?	

Section II: Mitigation	
Details of any compromised user accounts, including date of compromise and PIV enforced.	
Details of any new user accounts added to the computer, including date of addition.	

If blocks were implemented for foreign IP addresses, provide list with date/time implemented.	
Date suspicious files were disinfected, quarantined, deleted, and/or replaced:	
Date credentials were reset on compromised account(s):	Choose a Date
Date user was counseled about the policy violation:	Choose a Date
Describe the type of attack (i.e. Phishing, Port Scan, Network Mapping, etc.).	
Did the e-mail contain an attachment or URL? If so, provide details.	
Date the e-mail was quarantined or deleted from the user's inbox:	Choose a Date
If an email server is involved, list spam or malicious emails found.	
If activity is related to scanning/network mapping, provide start/end/duration times.	
Lost/Stolen Equipment	
Type of equipment (i.e. make, model, serial number, mobile phone number, IMEI #):	
Approximate value:	
Address where the incident occurred:	
Circumstances surrounding the incident:	
Was encryption software installed? If so, provide details.	
Was the equipment password protected?	
Date the equipment was remotely purged:	Choose a Date
Date of service or network access disconnection:	Choose a Date
If stolen, provide law enforcement agency, police report number and date filed.	

Section III: Root Cause	
Threat Vector: (Unknown, Attrition, Web, Email, External/Removable Media, Impersonation/Spoofing, Improper Usage, Loss or Theft of Equipment, Other)	Choose an item.
If Threat Vector is Other, provide details:	
What vulnerabilities were exploited?	
How could this incident have been prevented?	

Section IV: Additional Information

Provide anti-virus logs, firewall logs, screen captures, post scan logs and any additional information not included in previous sections: