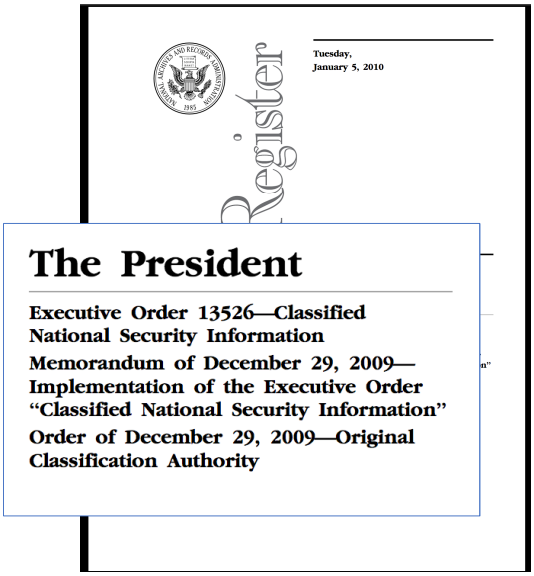


Tuesday,
January 5, 2010

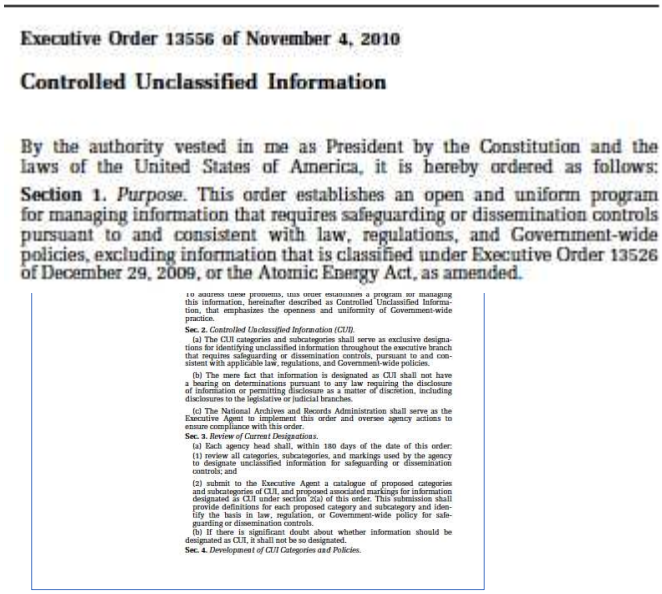
Register

The President

Executive Order 13526—Classified National Security Information

Memorandum of December 29, 2009—Implementation of the Executive Order "Classified National Security Information"

Order of December 29, 2009—Original Classification Authority



Executive Order 13556 of November 4, 2010

Controlled Unclassified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Purpose.* This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

OEMs and Federal Contractors

- References in subcontracts and purchase orders to any FAR clauses, which start with 52.2XX-XX
- References in subcontracts and purchase orders to any Department of Defense FAR Supplement (DFARS) clauses, which start with 252.2XX-XXXX, or other agency supplemental clauses
- Reference to a Defense Priorities & Allocations System Program (DPAS) rating
- Requirements to comply with the International Traffic in Arms Regulations (ITAR)
- Requirements to comply with NIST SP 800-53
- Requirements to comply with NIST SP 800-171r1

Controlled Unclassified Information (CUI) Registry

- Agriculture
- Controlled Technical Information
- Critical Infrastructure
- Emergency Management
- Export Control
- Financial
- Geodetic Product Information
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- NATO
- Nuclear
- Privacy
- Procurement and Acquisition
- Financial
- Proprietary Business Information
- SAFETY Act Information
- Statistical
- Tax
- Transportation

https://www.archives.gov/cui/registry/category-list#page-header

NIST SP 800-53 R4

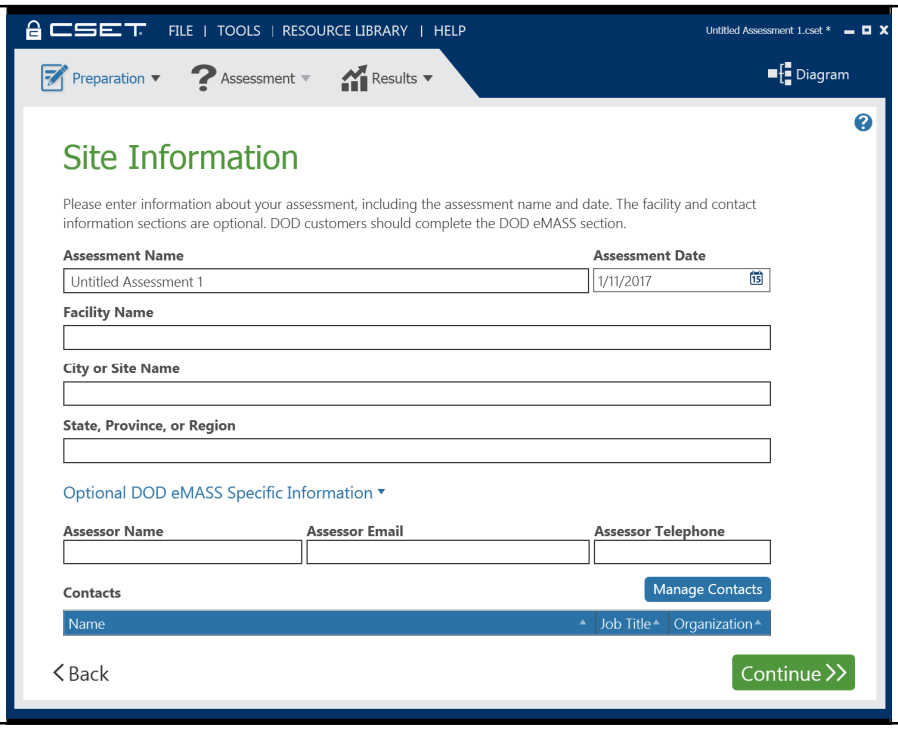
NIST 800-53 R4 Control Families			
AC	ACCESS CONTROL	MA	MAINTENANCE
AP	AUTHORITY AND PURPOSE	MP	MEDIA PROTECTION
AR	ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT	PE	PHYSICAL AND ENVIRONMENTAL PROTECTION
AT	AWARENESS AND TRAINING	PS	PERSONNEL SECURITY
AU	AUDIT AND ACCOUNTABILITY	PL	PLANNING
CA	SECURITY ASSESSMENT AND AUTHORIZATION	PM	PROGRAM MANAGEMENT
CM	CONFIGURATION MANAGEMENT	RA	RISK ASSESSMENT
CP	CONTINGENCY PLANNING	SA	SYSTEM AND SERVICES ACQUISITION
DI	DATA QUALITY AND INTEGRITY	SC	SYSTEM AND COMMUNICATIONS PROTECTION
DM	DATA QUALITY AND INTEGRITY	SE	SECURITY
IA	IDENTIFICATION AND AUTHENTICATION	SI	SYSTEM AND INFORMATION INTEGRITY
IP	INDIVIDUAL PARTICIPATION AND REDRESS	TR	TR-1
IR	INCIDENT RESPONSE	UL	USE LIMITATION
800-53 R4 Family Count = 26			

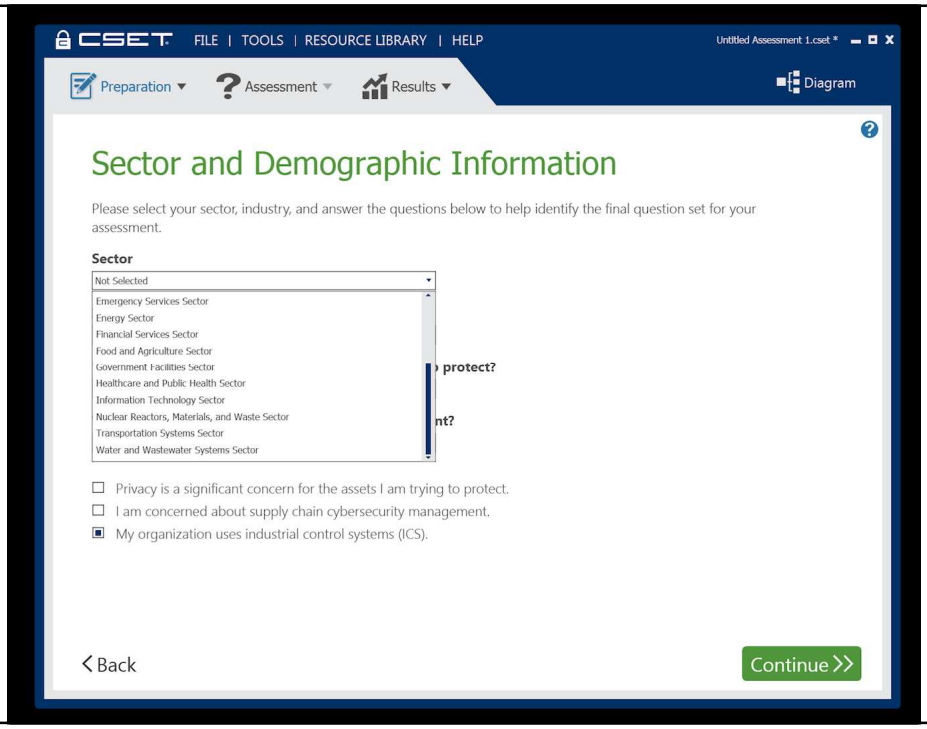
NIST SP 800-171R1

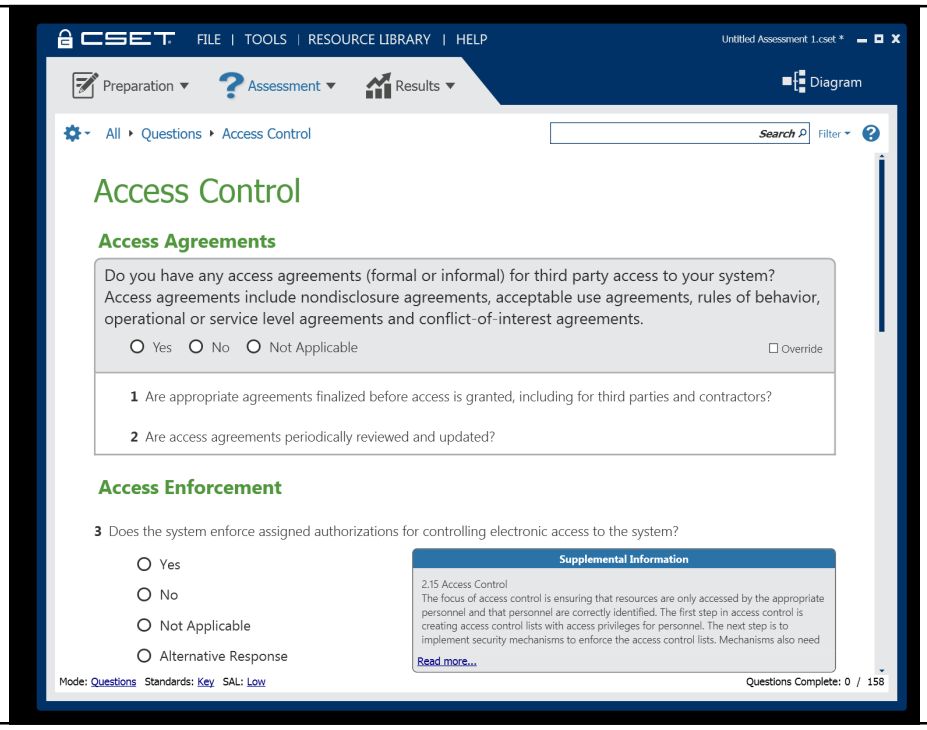
NIST 800-171 Families	
AC	ACCESS CONTROL
AT	AWARENESS AND TRAINING
AU	AUDIT AND ACCOUNTABILITY
CA	SECURITY ASSESSMENT
CM	CONFIGURATION MANAGEMENT
IA	IDENTIFICATION AND AUTHENTICATION
IR	INCIDENT RESPONSE
MA	MAINTENANCE
MP	MEDIA PROTECTION
PS	PERSONNEL SECURITY
PE	PHYSICAL PROTECTION
RA	RISK ASSESSMENT
SC	SYSTEM AND COMMUNICATIONS PROTECTION
SI	SYSTEM AND INFORMATION INTEGRITY
CP	CONTINGENCY PLANNING
SA	SYSTEM AND SERVICES ACQUISITION

DUE BY DECEMBER 31, 2017


CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
Untitled Assessment 1.cset
Preparation
Assessment
Results
Diagram
CSET®
CYBER SECURITY EVALUATION TOOL
Version 8.0
Prepare Your Assessment
CSET helps you determine the cybersecurity posture of your organization as you answer questions based on recognized industry standards about your systems and procedures.
Before you can answer questions, your question set needs to be identified. The 'Start Here' button begins the question identification and preparation process.
Start Here


CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
Untitled Assessment 1.cset *
Preparation
Assessment
Results
Diagram
Site Information
Please enter information about your assessment, including the assessment name and date. The facility and contact information sections are optional. DOD customers should complete the DOD eMASS section.
Assessment Name
Untitled Assessment 1
Assessment Date
1/11/2017
Facility Name
City or Site Name
State, Province, or Region
Optional DOD eMASS Specific Information
Assessor Name
Assessor Email
Assessor Telephone
Contacts
Manage Contacts
Name
Job Title
Organization
Back
Continue


CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
Untitled Assessment 1.cset *
Preparation
Assessment
Results
Diagram
Sector and Demographic Information
Please select your sector, industry, and answer the questions below to help identify the final question set for your assessment.
Sector
Not Selected
Emergency Services Sector
Energy Sector
Financial Services Sector
Food and Agriculture Sector
Government Facilities Sector
Healthcare and Public Health Sector
Information Technology Sector
Nuclear Reactors, Materials, and Waste Sector
Transportation Systems Sector
Water and Wastewater Systems Sector
protect?
nt?
Privacy is a significant concern for the assets I am trying to protect.
I am concerned about supply chain cybersecurity management.
My organization uses industrial control systems (ICS).
Back
Continue


CSET
FILE | TOOLS | RESOURCE LIBRARY | HELP
Untitled Assessment 1.cset *
Preparation
Assessment
Results
Diagram
All ▸ Questions ▸ Access Control
Search
Filter
Access Control
Access Agreements
Do you have any access agreements (formal or informal) for third party access to your system? Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, operational or service level agreements and conflict-of-interest agreements.
Yes
No
Not Applicable
Override
1 Are appropriate agreements finalized before access is granted, including for third parties and contractors?
2 Are access agreements periodically reviewed and updated?
Access Enforcement
3 Does the system enforce assigned authorizations for controlling electronic access to the system?
Yes
No
Not Applicable
Alternative Response
Supplemental Information
2.15 Access Control
The focus of access control is ensuring that resources are only accessed by the appropriate personnel and that personnel are correctly identified. The first step in access control is creating access control lists with access privileges for personnel. The next step is to implement security mechanisms to enforce the access control lists. Mechanisms also need
Read more...
Mode: Questions Standards: Key SAL: Low
Questions Complete: 0 / 158

Questions for OEM and Government Contractors

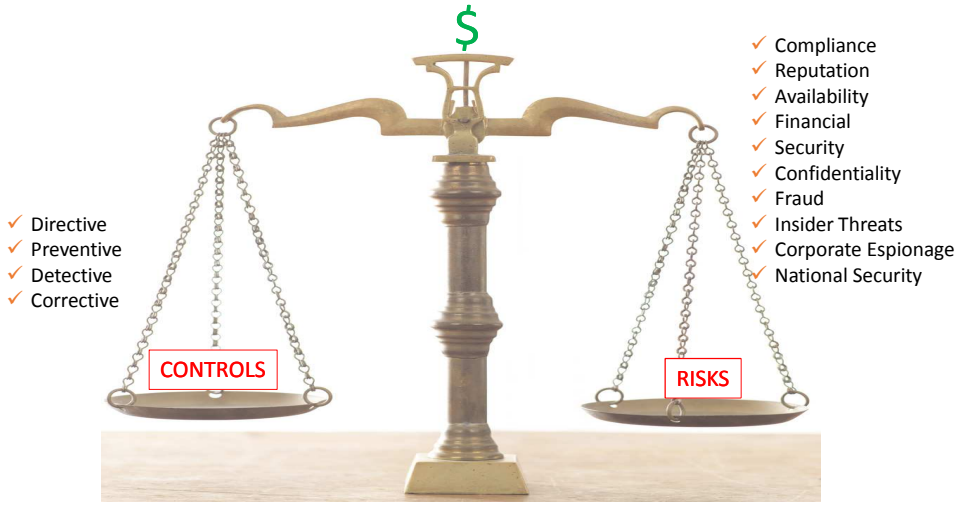
- What obstacles will you encounter from starting?
  - Cost?
  - Investments?
- What obstacles will you encounter from establishing actionable plan of action and milestones for cybersecurity (POAM)?
- What constraints control progress in Cyber programs?
  - Finding the right cyber certified provider?
  - Finding cost-effective initial solutions ? (in-house, outsource, managed services)
- What are the constraints to detection?

Supply Chain Information Security

The issues are mainly:

1. infrastructural issues – organization structure, technology competence, training, relationships with partners
2. strategy development parameters and issues – strategy for security information flow between organizations
3. local protocols issues – wireless, RFID, mobile devices
4. emerging technologies impacting the flow of information in the supply chain – Internet, satellite, EDI, robotics, ERP
5. power and control issues in inter-organizational systems – different perspectives from different stakeholders on who controls security within the supply chain

Balanced View of Information Security



MIGUEL (Mike) O. Villegas

Miguel (Mike) O. Villegas is a Vice President for K3DES LLC. He performs and QA's PCI-DSS and PA-DSS assessments for K3DES clients. He also manages the K3DES ISO/IEC 27002:2013 program. Mike was previously Director of Information Security at Newegg, Inc. for five years. Mike currently is a Contributing Writer for SearchSecurity.com -TechTarget.

Mike has over 35 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Arthur Andersen and Ernst & Young for their information systems security and IS audit groups over a span of nine years. Mike is a CISA, CISSP, GSEC, PCI-QSA and PA-QSA.

Mike was president of the LA ISACA Chapter during 2010-2012 and president of the SF ISACA Chapter during 2005-2006. He was the SF Fall Conference Co-Chair from 2002–2007 and also served for two years as Vice President on the Board of Directors for ISACA International. Mike has taught CISA review courses for over 20 years.