

### Best Practices and Vulnerabilities for Privileged Accounts

---

---

---

---

---

---

---

---



### Best Practices and Vulnerabilities for Privileged Accounts

NAVIGATION IN THE MEETING ROOM

Notes & Announcements

File Share

Q & A

Enlarge Screen

Poll #1

View Votes

How many s Process

- 3
- 4
- 5
- 6
- No Vote

Close Caption below

---

---

---


---

---

---

---


---



### Best Practices and Vulnerabilities for Privileged Accounts

#### Overview

- Define Privilege Account
- Identify Common Types of Privileged Accounts
- Identify Risks Associated with Privileged Accounts
- Discuss Some Best Practices



3

---

---

---



---

---

---

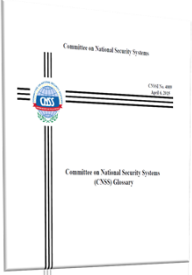
---

---

 **Best Practices and Vulnerabilities for Privileged Accounts** 

### Privileged User and Privileged Account

- **Privileged User**  
A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
- **Privileged Account**  
An information system account with approved authorizations of a privileged user.



4

---

---

---



---

---

---

---

---

 **Best Practices and Vulnerabilities for Privileged Accounts** 

### Responsibilities

**Privileged Users** (e.g., System Administrators) must:

- Configure and operate IT within the authorities vested in them according to DoD cybersecurity policies and procedures.
- Notify the responsible ISSO or, in the absence of an ISSO, the responsible ISSM, of any changes that might affect security posture.

IAW DoD 8500.01, March 14, 2014

5

---

---

---



---

---

---

---

---

 **Best Practices and Vulnerabilities for Privileged Accounts** 

### Workforce Categories and Specialties

**Category**

- IA Workforce Technical
  - IAT I
  - IAT II
  - IAT III
- IA Workforce Management
  - IAM I
  - IAM II
  - IAM III

**Specialty**

- Computer Network Defense Service Providers (CND-SPs)
- IA System Architects and Engineers (IASAEs)

6

---

---

---

---

---

---

---

---

Privileged Users

### QUALIFICATIONS

Personnel filling positions with privileged access must satisfy both preparatory and sustaining DOD IA training and certification requirements

Table AP3.T2  
DoD Approved  
Baseline Certifications

IAI Level I		IAI Level II		IAI Level III	
A+ CE Network+ CE SSCP <i>CISSA Security</i>	OSSEC Security+ CE SSCP <i>CISSA Security</i>	CISA GSEC CISAP <i>CISSP (or Associate)</i>	GCN GCEC CISAP <i>CISSP (or Associate)</i>		
IAM Level I		IAM Level II		IAM Level III	
CAP OSBP GSLC Security+ CE	CAP GSLC CISM CASP CISSP (or Associate)			GSLC CISM CISSP (or Associate)	
IASAE I		IASAE II		IASAE III	
CISSP (or Associate) CASP CISLP	CISSP (or Associate) CASP CISLP			CISSP - ISSEP CISSP - ISSAP	
CDSP Infrastructure Support		CDSP Incident Response		CDSP Auditor	
GCIA CEH GCIH	SSCP CEH	GCN CSM CEH <i>GCFA</i>	CISA GSNA CEH	CISSP-DSMP CISM	

---

---

---

---

---

---

---

---

---

---

---

---

Best Practices and Vulnerabilities  
for Privileged Accounts

### Polling Question 1:

Do you believe that privilege users pose a threat in your organization?

Yes

No

---

---

---

---

---

---

---

---

---

---

---

---

Best Practices and Vulnerabilities  
for Privileged Accounts

### Cyber Attacks

**Database admin steals 2.3M consumer records at Fidelity National subsidiary**

The data includes names, addresses, birth dates, and other identifying information.

**Medco sys admin gets 30 months for planting logic bomb**

Medco attorneys could have originated plaintiffs' ability to check for deadly drug interactions, U.S. attorney says

**Edward Snowden Leaked Thousands of NSA Documents**

**San Francisco IT worker arrested in hijacking of city network**

Disgruntled city worker in jail on \$5 million bail after allegedly locking administrators out of the city's wireless area network.

---

---

---

---

---

---

---

---

---

---

---

---

**Best Practices and Vulnerabilities for Privileged Accounts** **CDSE**

U.S.  
**Attack Gave Chinese Hackers Privileged Access to U.S. Systems**  
By BARBARA HANSEN, NICOLE PEARSON and MICHAEL S. HIGLEY, JCS, et al.



Secretary of Defense, Board of the Office of Personnel Management, in Congress on Tuesday, 10/14/2013. Associated Press

10

---

---

---

---

---

---

---

---

**Best Practices and Vulnerabilities for Privileged Accounts** **CDSE**

**Common Privileged Accounts**

- System Administrator Account
- Database Administrator Account
- Web Administrator Account
- Network Administrator Account
- Application Developer Account
- System Accounts
- Service Accounts

11

---

---

---

---

---

---

---

---

**Best Practices and Vulnerabilities for Privileged Accounts** **CDSE**

**Service Accounts**

Consider using

- LocalService
- NetworkService

12

---

---

---

---

---

---

---

---

Best Practices and Vulnerabilities for Privileged Accounts CDSE

**Poll Question 2:**

At a minimum, how often should privileged accounts passwords be changed?

- 30 days
- 60 days
- 90 days

13

---

---

---

---

---

---

---

---

Best Practices and Vulnerabilities for Privileged Accounts CDSE

**PASSWORDS**

Sorry, but your password must contain at least an uppercase letter, a lowercase letter, a number, and a special character.



14

---

---

---

---

---

---

---

---

Best Practices and Vulnerabilities for Privileged Accounts CDSE

**Privileged Users Should**

**NEVER**

Use Privilege Accounts to Perform Day to Day Functions



15

---

---

---

---

---

---

---

---

Best Practices and Vulnerabilities for Privileged Accounts CDSE



16

---

---

---

---

---

---

---

---

Best Practices and Vulnerabilities for Privileged Accounts CDSE

**Least Privileges**  
Grant individuals access to only those specific resources and functions required to carry out their current responsibilities

**ACCESS DENIED:**  
The Principle of Least Privilege



17

---

---

---

---

---


---

---

---

Best Practices and Vulnerabilities for Privileged Accounts CDSE

**Separation of Duties**  
Divide roles and responsibilities among multiple people to exclude the ability of one person to perform all privilege actions on a system



18

---

---

---

---

---

---

---

---

**Best Practices and Vulnerabilities for Privileged Accounts** CDSE

---

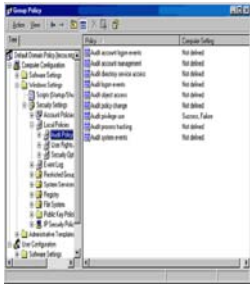
### Audit Privileged Use

**Auditing Successes**

- Generates an audit entry when the exercise of a privileged user right succeeds

**Auditing Failures**

- Generates an audit entry when the exercise of a privileged user right fails



---

---

---

---

---

---

---

---

---

---

**Best Practices and Vulnerabilities for Privileged Accounts** CDSE

---

### Audit "Sensitive Privilege Use"

- Act as part of the operating system
- Back up files and directories
- Create a token object
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Generate security audits
- Impersonate a client after authentication
- Load and unload device drivers
- Manage auditing and security log
- Modify firmware environment values
- Replace a process-level token
- Restore files and directories
- Take ownership of files or other objects

---

---

---

---

---

---

---

---

---

---

**Best Practices and Vulnerabilities for Privileged Accounts** CDSE

---

### Policy

Develop a policy that defines how privileged accounts will be managed.



---

---

---

---

---

---

---

---

---

---



**Best Practices and Vulnerabilities for Privileged Accounts**



**Conclusion**




---

---

---

---

---

---

---

---



**Best Practices and Vulnerabilities for Privileged Accounts**



**Available Education and Training**

Center for Development of Security Excellence  
DEPARTMENT OF DEFENSE  
**DEFENSE SECURITY SERVICE**

Home | About Us | Publications | Services | Information Systems | Contact Us

**CDSE**

**Center for Development of Security Excellence**  
Education, training, and professional services for the Department of Defense and Industry

**SPED**  
Specialty level security professional certification

**SPED**  
Specialty level security professional certification

**Access Security Professional Education (ASPE)**  
Take courses specifically designed to prepare DoD security specialists for leadership positions and responsibilities.

- Education Programs
- College-level and Graduate Courses
- Certification
- FAGS

**Connect to SPED Certification**

- Learn About SPED Certification
- Request an Inbound SPED Credit
- Prepare for SPED Certification
- Obtain Your SPED Certification
- Recur Your SPED
- More SPED Resources for both Component and DoD

**Access Security Training & Job Aids (ASJA)**  
Access our course catalog to view security courses in a variety of formats:

- Instructional DVD
- Workshop
- Webinars
- Job Aids
- Books
- Posters
- Slides

**Access Toolkits (AT)**  
ATKit are a repository of role-based resources that serve as a one-stop shop for security professionals.

- Cybersecurity Professional
- Information System Security Manager (ISSM)
- Security Education and Training, Awareness (SETA) Professional

**CDSE News/Events**

August 18, 2014 - **How to Grow, Set, and Measure Metrics and Personal Security Awareness Goals**

August 18, 2014 - **How to Grow, Set, and Measure Metrics and Personal Security Awareness Goals**

August 11, 2014 - **Information Systems Security Awareness (ISSA) 2014**

23

---

---

---

---

---

---

---

---



**Best Practices and Vulnerabilities for Privileged Accounts**



**Questions**



24

---

---

---

---



---

---

---

---



 **Best Practices and Vulnerabilities for Privileged Accounts** 

**Feedback**

Before we conclude today's presentation, we hope you'll take a moment to participate in our feedback questionnaire. Your feedback is very helpful to us and is greatly appreciated. If you have ideas for future webinar topics, you're able to share these in the questionnaire.

25

---

---

---

---

---

---

---

---

 **Best Practices and Vulnerabilities for Privileged Accounts** 

**Cybersecurity Training Products and POC**

**Past Webinars**

- [Information Security Continuous Monitoring](#)
- [Monthly Cyber Awareness](#)
- [Trusted Downloading](#)
- [NISP C&A Process and OBMS](#)

**All Other Training**

- [CDSE Cybersecurity](#)

Renee Hartsfield  
Work: (410) 689-1373

E-mail:  
dorothy.hartsfield@dss.mil  
cybersecurity.training@dss.mil

26

---

---

---

---

---

---

---

---