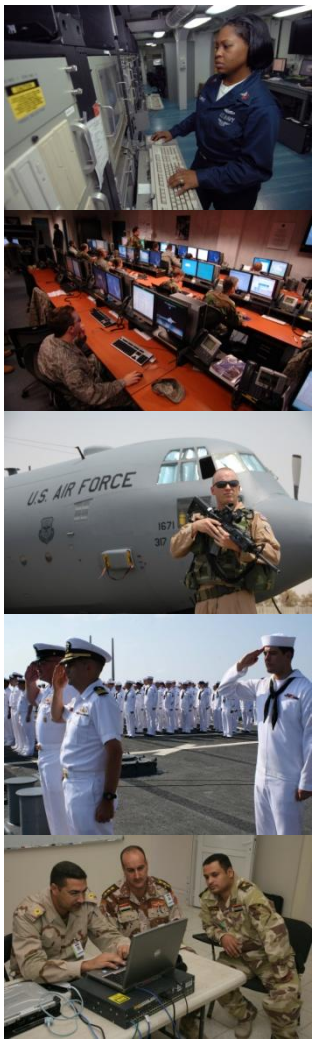
# DIACAP Compliance

# Enterprise Random Password Manager

## Introduction

Lieberman Software's Privileged Identity Management solutions help federal government organizations comply with the DoD Information Assurance Certification and Accreditation Process (DIACAP). To ensure that risk management is applied on information systems, DIACAP defines a standard set of controls, tasks and activities for the enforcement and ongoing maintenance of Information Assurance policies.

## What We're Hearing From DoD Customers




Our DoD customers tell us that Lieberman Software's **Enterprise Random Password Manager (ERPM)** addresses three very specific areas of DIACAP compliance:

1. **DoD password length policy** states mandatory 15 character password length for all accounts. Microsoft AD/Group policy will only enforce up to 14 characters. ERPM will allow you to set password length policies outside of AD so you can achieve the 15 character password requirement – ERPM allows 127 characters.

2. **DoD password complexity requirement** is to have one (or more) of all four categories enforced: **upper case character, lower case character, number, AND special character**. Microsoft AD/Group policy settings for password complexity will only enforce three out of the four categories: upper, lower, number, **OR** special. The only way to accomplish DoD password complexity requirements would be to write a custom DLL to enforce this through group policy or to use ERPM.

3. **Service account passwords must be changed once a year** (minimally). With ERPM, managing service accounts is much easier and more efficient than using manual processes. Having an automated solution is better than writing a script that may or may not work; and, ERPM propagates all password changes to everywhere service accounts are in use so nothing breaks.

www.liebsoft.com | P 800.829.6263 (USA/Canada) P (01) 310.550.8575 (Worldwide) F (01) 310.550.1152 | 1900 Avenue of the Stars, Suite 425, Los Angeles, CA 90067
© 2011 Lieberman Software Corporation. Trademarks are the property of their respective owners.

## ERPM and DIACAP Information Assurance Controls

The DIACAP requirements include specifications for dealing with Privileged Users and securing access to privileged assets. In particular, ERPM – Lieberman Software's Privileged Identity Management solution – addresses the following DIACAP Information Assurance (IA) Controls:

| IA Control Subject Area | IA Control # | IA Control Name | Relevant IA Control Text |
|---|---|---|---|
| Identification and Authentication Confidentiality | IAGA-1 | Group Identification and Authentication | Group authenticators for application or network access may be used only in conjunction with an individual authenticator. |
| | IAIA-2 | Individual Identification and Authentication | DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user logon ID) and password. |
| Identification and Authentication Integrity | IATS-2 | Token and Certificate Standards | Identification and authentication is accomplished using the DoD PKI Class 3 or 4 certificate (NIST FIPS 140-2 validated cryptography) and hardware security token (when available). System mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse, and processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password. All factory set, default or standard-user IDs and passwords are removed or changed. Passwords are encrypted both for storage and for transmission. |
| Enclave and Computing Environment Confidentiality | ECAN-1 | Access for Need-to-Know | Controlled access to information that is made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction. All access to need-to-know information and all failed access attempts are recorded in audit transactions. |


© 2011 Lieberman Software Corporation. Trademarks are the property of their respective owners.

| IA Control Subject Area | IA Control # | IA Control Name | Relevant IA Control Text |
|---|---|---|---|
| Enclave and Computing Environment Integrity | ECAR-3 | Audit Record Content | Audit records include privileged activities and other system-level access. |
| | ECAT-2 | Audit Trail, Monitoring, Analysis and Reporting | Automated, continuous on-line monitoring and audit trail creation; immediately alert personnel of any unusual or inappropriate activity. |
| | ECCD-2 | Changes to Data | Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel. Access and changes to the data are recorded in transaction logs that are reviewed periodically or immediately upon system security events. |
| | ECND-2 | Network Device Controls | Protection from deletion of system and application files; Audit or other technical measures are in place to ensure that the network device controls are not compromised. |
| | ECPA-1 | Privileged Account Control | All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles. The IAM tracks privileged role assignments. |
| | ECRG-1 | Audit Reduction and Report Generation | Tools are available for the review of audit records and for report generation from audit records. |
| | ECTP-1 | Audit Trail Protection | The contents of audit trails are protected against unauthorized access, modification or deletion. |
| Enclave and Computing Environment | ECLP-1 | Least Privilege | Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. |


© 2011 Lieberman Software Corporation. Trademarks are the property of their respective owners.

## About Enterprise Random Password Manager (ERPM)

ERPM is the privileged identity management solution that automatically discovers, strengthens, monitors and recovers local, domain and process account passwords in the cross-platform enterprise. It helps you achieve full compliance with your security and operational auditor's privileged account password management and shared account password management requirements.

ERPM identifies, safeguards (stores in a database using FIPS 140-2 encryption) and manages the privileged identities found throughout your infrastructure, including:

- **Super-user login accounts** utilized by individuals to change configuration settings, run programs and perform other administrative duties. These accounts exist on virtually every server and desktop operating system, business application, database, Web service, and network appliance in your organization.
- **Service accounts** that require privileged login IDs and passwords to run.
- **Application-to-application passwords,** the credentials used by web services, line-of-business applications, custom software, and virtually every other type of application to connect to databases, middleware, and other application tiers.

ERPM then propagates secure, frequently changed passwords to each location and grants fast, audited access to authorized IT staff whenever they need to perform routine maintenance or emergency firecall repairs.

## About Lieberman Software

Lieberman Software provides privileged identity management solutions to secure the world's largest cross-platform enterprises and governments, having pioneered the first product to address this need in 1999. By automating time-intensive administration tasks, Lieberman Software increases control over the IT infrastructure, reduces security vulnerabilities, improves productivity and ensures regulatory compliance.

A managed Microsoft Gold Certified Partner and Oracle Platinum Partner, Lieberman Software has integration partnerships with leading technology vendors including ArcSight, BMC, Cisco, Dell, Hewlett-Packard, IBM, Intel, Novell, ObserveIT, Q1 Labs, Raytheon, Red Hat, RSA, Sybase and Thales.

The company holds multiple Gov/MIL compliance accreditations including the US Army Certificate of Networthiness (CoN). It has reseller and systems integrator partners with Certified Disabled Veteran and National Minority Supplier status.

The company is headquartered in Los Angeles, CA and maintains a regional office in Austin, TX. All product development, testing, and support operations are based in the United States. For more information, please visit the company website: **www.liebsoft.com.**


© 2011 Lieberman Software Corporation. Trademarks are the property of their respective owners.