Keeping Up with Federal Requirements

Cybersecurity and the Competitive Edge

Leon Jaimes

leon@sollievoit.com
www.sollievoit.com
● Improving cybersecurity is a competitive advantage.

● Benefits & Consequences
Improving cybersecurity is a competitive advantage.

Many benefits in addition to consequences.
Benefits

- Positive reputation as a secure company
- Threats are getting worse
- Cybersecurity program == accounting program
- Realize operational efficiencies sooner
- Last one standing when others fall
- Positive performance reviews
- Good for country

Leon Jaimes [leon@sollievoit.com]
Consequences

- DFARS Non-Compliance
- Negative Reputation
- Loss of IP and Work Product
- Breach of Contract Lawsuits
- Proposal Exclusion
- Adverse Performance Review
- Termination for Default
- Criminal Fraud
- False Claims Act Actions
Defense Acquisition Regulation Supplement (DFARS) clause 252.204-7012 and NIST SP 800-171 High Level
This about....
Defending the Nation
DFARS
“weaponized”
800-171
Do not ignore; not going to go away.

January 21, 2019

Under Secretary for Defense Ellen M. Lord issued a memo stating her intent for DCMA to audit the DoD supply chain for DFARS compliance.
Defense Contract Management Agency (DCMA) is not going to assess compliance against the NIST SP800-171 controls...

They will be looking for SSPs and POAs
Provide adequate security to safeguard covered defense information
Requirements
Rapidly report cyber incidents to DoD

Within 72 hours
Submit malicious software samples to DoD
Preserve and protect evidence for at least 90 days
A Few Key Terms
CUI - Controlled Unclassified Information

- CUI that you are given by the government that is marked as CUI, or
- CUI that you are creating for the government that is designated as CUI
CDI - Covered Defense Information

- Information that requires protection under DFARS Clause 252.204-7012.
- Unclassified controlled technical information (CTI) or other information, as described in the CUI Registry, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies and...
• Is marked or otherwise identified in the contract, task order, or delivery order and provided to contract, task order, or delivery order and provided to contractor by or on behalf of, DoD in support of the performance of the contract; or...
Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract.
Organizational Systems

- Systems that protect systems that process, store, or transmit CUI, and
- Systems that process, store, or transmit CUI.
SP 800-171

14 families/categories of controls

They are all important, but audit is really important.

244 (CUI) + 63 (NFO) controls
A contractor may use a SSP to document implementation of the NIST SP 800-171 security requirements. DoD organizations might choose to leverage the contractor’s SSP, and any associated POA, in the contract formation, administration, and source selection processes.
RISK
Threat - Vulnerability - Impact - Likelihood

• In today's world that **Likelihood** is less and less important because there is almost a 100% likelihood that your either have been hit or you're going to be.

• Complexity is the greatest threat.

*Dr. Ron Ross - NIST Fellow - 10/18/2018*
Anatomy of Supply Chain Attack

Leon Jaimes [leon@sollievoit.com]
“America’s Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It” - WSJ Jan. 10th, 2019
● Website or web server hacked

Leon Jaimes [leon@sollievoit.com]
• The visitors to the original website were hacked
• Additional hacked website used to phish
• Hacked accounts or systems were used to attack multiple other businesses

Leon Jaimes [leon@sollievoit.com]
● Multiple businesses attack even more businesses
● Orchestrated attacks converge on target utility companies
Elements of the Attack

● Small Businesses
  ○ At least 28 entities with known relationship to the attack campaign
  ○ Multiple small businesses, 1-20 employees were used as the starting point of the attack
  ○ Attackers attacked the same small businesses multiple times
  ○ Attackers either persisted, or re-compromised at least one company

● Timeline
  ○ Summer 2016 to at least Fall 2018

● Utilities
  ○ At least 60 utilities were targeted
  ○ At least 24 were breached
  ○ 8 utilities were penetrated far enough for attackers to reach the control systems

● Attack Methods
  ○ Email Phishing / Spear Phishing
  ○ Compromised Websites / Watering Hole
  ○ Malicious Attachments
A mess
“Cybercriminals are still finding success with the same tried and tested techniques, and their victims are still making the same mistakes.”


Leon Jaimes [leon@sollievoit.com]
The unfortunate reality is that this is probably your company.

8 of 8 of our network penetration testing engagements in the last two years were successful in achieving full compromise.
How we are successfully attacking networks

Leon Jaimes [leon@sollievoit.com]
Establish a Foothold

- Wireless - *Physical proximity*
- Phishing - *Anywhere*
- Exploit Public Facing Vulnerable Systems - *Anywhere*
- Weak / Known Passwords - *Anywhere*
Wireless

Leon Jaimes [leon@sollievoit.com]
Once Inside...Attack

- Unpatched Systems
- Unsegmented Networks
- Inadequate Detection and Response
- Credential Mismanagement
- Excessive Privileges
- * Not Advanced Persistent Threats (APTs) or 0-days

Leon Jaimes [leon@sollievoit.com]
Full Compromise

- Establish Persistence
- Steal Sensitive Data
- Drain the Bank Accounts
- Compromise Business Partners
- Delete Backups, and Backups of Backups

Leon Jaimes [leon@sollievoit.com]
DFARS 252.204-7012 and NIST SP 800-171 Additional Details
DFARS 7012

- Contractors and subs must comply with NIST SP 800-171
- Prime - Report all cybersecurity incidents to the DoD within 72 hours
- Subs - Report all cybersecurity incidents to the Prime/next tier within 72 hours
- Submit evidence to DoD

Leon Jaimes [leon@sollievoit.com]
DFARS 7012

- Goals
  - Proactive
  - Prevent supply chain attacks
  - Detect and respond to attacks
  - Capture and share evidence from attacks
NIST SP 800-171

- 800-171 - 3.12.4 - Describe in a system security plan (SSP), how the specified security requirements are met or the plan for how they will be met
- 800-171 - 3.12.2 - Develop and implement Plans of Action (POA) & Milestones (&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in systems

Leon Jaimes [leon@sollievoit.com]
NIST SP800-171

- Basic & Derived Requirements.
  - Basic security requirements - High level, obtained from FIPS 200
  - Derived security requirements - Supplement the basic security requirements. Taken from detailed controls in NIST SP800-53.

Leon Jaimes [leon@sollievoit.com]
NIST SP800-171

- February 2018 updates
  - “The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components”
  - 24 of the 30 substantive changes are around the AU (Audit and Accountability) requirements.
  - Clarification with verbiage around "audit" vs. "capture" and "log".

Leon Jaimes [leon@sollievoit.com]
NIST SP800-171

- June 2018 updates
  - Appendix F - Discussion - ~40 pages of discussion and clarification around each of the controls
  - Definition of a security domain
NIST SP800-171

- Revision 2 is coming soon - by the end of the month for public review
- It looks like it may be expanded to all federal contractors, and universities
Challenges
- Financial
- People
- Technical
Financial $$

1. $ hardware and software
2. $ salaries
3. $ breach/incident insurance
4. $ audits / services
People

1. Retraining
2. Awareness training
3. Incentivizing and motivating
4. Hiring
Technical

1. Inventory
2. Vulnerability monitoring and remediation
3. Adversaries
4. Evolution
5. Technical Debt

Do we need a WAF, an IPS, a malware gateway, a URL filter, a SPAM filter, a sandbox, next gen endpoint protection, UEBA, SOAR, data science, CASB, MDR, EDR, SOC, SIEM, dynamic analysis, static analysis, Trevor?

Leon Jaimes [leon@sollievoit.com]
Free (aka low cost) Tools!
CSET

CSET is a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems. The tool derives the recommendations from a database of cybersecurity standards, guidelines, and practices. Each recommendation is linked to a set of actions that can be applied to enhance cybersecurity controls.

https://cset.inl.gov/SitePages/Home.aspx
Audit, Audit, Audit

There is a reason that there were nine “Substantive” changes involving auditing in NIST Special Publication 800-171 Revision 1...Feb. 2018

Easily tie this into most stages of Incident Response frameworks;

- Planning
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Leon Jaimes [leon@sollievoit.com]
Logging Solutions

1. Firewalls
2. Domain Controllers
3. DNS Servers
4. DHCP Servers
5. Web Servers
6. Network Flows
7. Rolling PCAPs
LAPS (Local Administrator Password Solution)
Windows Firewall

- Spend some time *architecting* the host based firewall.
- Deploy through GPOs.
- Stop turning it off on servers.
- Does Windows Firewall count as network segmentation?

Leon Jaimes [leon@sollievoit.com]
Bloodhound
Developed by @_wald0, @CptJesus, and @harmj0y.

Clean up that steaming pile of privileged users and ACLs.

Leon Jaimes [leon@sollievoit.com]
Nzyme; WiFi Monitoring, Intrusion Detection And Forensics
Domain Admin Canary Account

Leon Jaimes [leon@sollievoit.com]
Recon yourself / your company

- Shodan.io
- Censys.io
- Have I Been Pwned
- Pastebin
- Google
Long Term Success
Policies, Processes, and Procedures

Lots of fill-in-the-blanks in the controls.

Leon Jaimes [leon@sollievoit.com]
Nobody *wants* their job to be more difficult.

Leon Jaimes [leon@sollievoit.com]
Bring People Along - It's Important!

- No matter what the position in the organization, or in society, in nearly every case, it will have some form of information security task or responsibility.
- The broader the involvement, the better.
- Person as a sensor.
Allow Room for the Reactive and Unplanned

Leon Jaimes [leon@sollievoit.com]
Identify Planned Work

- Inventory planned work as things progress.
- Add to the inventory
- Track actual time against estimates.
- Use this data to develop run books.
- Use the data to budget and forecast.

“Meaningless statistics were up one-point-five per cent this month over last month.”

Leon Jaimes [leon@sollievoit.com]
Conclusions
Cybersecurity is a Competitive Advantage and Critical to National Security
DFARS Cybersecurity requirements are here to stay. More are coming, and the scope is growing.
Help is available

- PTAC
- NIST
- CUI Registry
- MEP / MAKE
- Contracting Office
- Prime
- Sollievo IT
Thank You!

Leon Jaimes - Sollievo IT, LLC - @slyride - leon@sollievoit.com
Improving cybersecurity is a competitive advantage

❖ Benefits

➢ Reputation as a secure company
➢ Threats are getting worse
➢ A mature cybersecurity program is as standard to business as accounting

Leon Jaimes [leon@sollievoit.com]
Improving cybersecurity is a competitive advantage

❖ Benefits (cont.)

➢ Realize operational efficiencies sooner
➢ Last one standing when other fall
➢ Positive Performance Review
➢ Good for country

Leon Jaimes [leon@sollievoit.com]
Improving cybersecurity is a competitive advantage.

❖ Consequences
➢ DFARS - Required
➢ Reputation
➢ Lost IP and work product
➢ Breach of Contract Lawsuits
Improving cybersecurity is a competitive advantage.

❖ Consequences (cont.)
➢ Proposal Exclusion
➢ Adverse Performance Review
➢ Termination for Default
➢ Criminal Fraud
➢ False Claims Act Actions
Starting points to collect logs from

1. Firewalls
2. Domain Controllers
3. DNS Servers
4. DHCP Servers
5. Web Servers
6. Network Flows
7. Rolling PCAPs
RSYSLOG - www.rsyslog.com

Leon Jaimes [leon@sollievoit.com]
Quick Values for `flow_dst_port`

- **Value**: 445
- **%**: 100.00%
- **Count**: 242,540

Found 242,540 messages with field `Mendal_flow_dst_port`.

Histogram:

- 20,351 messages on Friday 23 September 2016, 00:10 - 00:00

Leon Jaimes [leon@sollievoit.com]
Log all kinds of very useful information from computer systems.

- Logs process creation with **full command line** for both current and parent processes.
- **Records the hash of process image files using SHA1** (the default), MD5, SHA256 or IMPHASH.
- Includes a process GUID in process create events to allow for correlation of events even when Windows reuses process IDs.
- Include a session GUID in each events to allow correlation of events on same logon session.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Logs opens for raw read access of disks and volumes
- Optionally **logs network connections, including each connection’s source process, IP addresses, port numbers, hostnames and port names.**
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Automatically reload configuration if changed in the registry.
- **Rule filtering to include or exclude certain events dynamically.**
- **Generates events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.**

Leon Jaimes [leon@sollievoit.com]
@SwiftOnSecurity put out an awesome Sysmon template pack:
https://github.com/SwiftOnSecurity/sysmon-config

Create your own and share them with others.
Free to search a single IP. $50 to get filters and API access. Students can get a discount.

This is a query using filters….

state:AK org:"GCI Communications" port:10001 -("New CPE")

https://www.shodan.io/search?query=state%3AAK+org%3A%22GCI+Communications%22+port%3A10001+-(%22New+CPE%22)

Shows 1,169 of these GCI devices listening on port 10001 in Alaska. Most are Ubiquiti wireless devices. Suspect these are Wireless ISP services for rural areas without copper/fiber.
- First Name
- Last Name
- Middle Initial
- Phone Number
- Spouse Name
- MAC address
- Internal IP address
- Public IP address
- Account #?
- Mostly rural areas...
Google Search

inurl:gci.com filetype:xlsx


This looked interesting
<table>
<thead>
<tr>
<th>Personal Name</th>
<th>Personal Email</th>
<th>Personal Referral</th>
<th>Personal Relationship</th>
<th>Hire Date</th>
<th>Hire Location</th>
<th>Hire Consultant</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joe Henderson</td>
<td><a href="mailto:shaw@llc.co">shaw@llc.co</a></td>
<td>Employee Referral</td>
<td>If you selected Other, please specify</td>
<td>18-Jan-16</td>
<td>Desal</td>
<td>Joe Henderson</td>
<td></td>
</tr>
<tr>
<td>Bob Smith</td>
<td><a href="mailto:bsmith@llc.co">bsmith@llc.co</a></td>
<td>Employee Referral</td>
<td>If you selected Other, please specify</td>
<td>07-Jan-16</td>
<td>Desal</td>
<td>Joe Henderson</td>
<td></td>
</tr>
<tr>
<td>Jane Doe</td>
<td><a href="mailto:jdoe@llc.co">jdoe@llc.co</a></td>
<td>Employee Referral</td>
<td>If you selected Other, please specify</td>
<td>10-Jan-16</td>
<td>Desal</td>
<td>Joe Henderson</td>
<td></td>
</tr>
<tr>
<td>David Lee</td>
<td><a href="mailto:dlee@llc.co">dlee@llc.co</a></td>
<td>Employee Referral</td>
<td>If you selected Other, please specify</td>
<td>20-Jan-16</td>
<td>Desal</td>
<td>Joe Henderson</td>
<td></td>
</tr>
<tr>
<td>Mary Johnson</td>
<td><a href="mailto:mjohnson@llc.co">mjohnson@llc.co</a></td>
<td>Employee Referral</td>
<td>If you selected Other, please specify</td>
<td>05-Jan-16</td>
<td>Desal</td>
<td>Joe Henderson</td>
<td></td>
</tr>
<tr>
<td>Bill Brown</td>
<td><a href="mailto:bbrown@llc.co">bbrown@llc.co</a></td>
<td>Employee Referral</td>
<td>If you selected Other, please specify</td>
<td>15-Jan-16</td>
<td>Desal</td>
<td>Joe Henderson</td>
<td></td>
</tr>
<tr>
<td>Sarah Wilson</td>
<td><a href="mailto:swilson@llc.co">swilson@llc.co</a></td>
<td>Employee Referral</td>
<td>If you selected Other, please specify</td>
<td>10-Jan-16</td>
<td>Desal</td>
<td>Joe Henderson</td>
<td></td>
</tr>
<tr>
<td>Michael Lee</td>
<td><a href="mailto:mlee@llc.co">mlee@llc.co</a></td>
<td>Employee Referral</td>
<td>If you selected Other, please specify</td>
<td>05-Jan-16</td>
<td>Desal</td>
<td>Joe Henderson</td>
<td></td>
</tr>
<tr>
<td>John Davis</td>
<td><a href="mailto:jdavis@llc.co">jdavis@llc.co</a></td>
<td>Employee Referral</td>
<td>If you selected Other, please specify</td>
<td>10-Jan-16</td>
<td>Desal</td>
<td>Joe Henderson</td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td>Last name</td>
<td>Additional information (e.g., Employee Name, Employee Referral, Employee Email)</td>
<td>Have You Ever Been Directly</td>
<td>How Did You Hear About GC?</td>
<td>If you wrote for</td>
<td>Referral Email</td>
<td>Job Code &amp; Title</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
<td>---------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Ronald</td>
<td>Barfield</td>
<td>[Employee Name: Employee Referral: Employee Email]</td>
<td>No</td>
<td>No</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>149</td>
<td>Joshu</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>No</td>
<td>No</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>210</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>No</td>
<td>No</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>211</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>212</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>213</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>214</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>215</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>216</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>217</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>218</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>219</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>220</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
<tr>
<td>221</td>
<td>Joshua</td>
<td>Berry [Friend Referral: Friend Referral: Friend Email]</td>
<td>Yes</td>
<td>Yes</td>
<td>Directly</td>
<td>[Referral Email]</td>
<td>[Job Code &amp; Title]</td>
</tr>
</tbody>
</table>

Google Search - “That’s what friends are for”
<table>
<thead>
<tr>
<th>Name</th>
<th>Title/Role</th>
<th>Action</th>
<th>Amount</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Philip Taylor</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>JobBoardsJobBoards</td>
</tr>
<tr>
<td>aganMorale</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Richard Lewis</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>JobBoardsJobBoards</td>
</tr>
<tr>
<td>Robert Elmore</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>GCCareerWebsite</td>
</tr>
<tr>
<td>Mohammed</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>New</td>
<td></td>
<td>Google Search</td>
</tr>
<tr>
<td>Allison Strickland</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>Yes</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Bradley</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>JobBoardsJobBoards</td>
</tr>
<tr>
<td>Bradley</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>Yes</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Bradley</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>Yes</td>
<td></td>
<td>OtherOther</td>
</tr>
<tr>
<td>Richard Lewis</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>JobBoardsJobBoards</td>
</tr>
<tr>
<td>Catherine Rogers</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>Yes</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Charles Swartz</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>OtherOther</td>
</tr>
<tr>
<td>Christopher Womack</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>JobBoardsJobBoards</td>
</tr>
<tr>
<td>Elena Bermanbl</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>GCCareerWebsiteGC</td>
</tr>
<tr>
<td>Elizabeth O'Brien</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>OtherOther</td>
</tr>
<tr>
<td>Esther Eastola</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Eugenia Taubad</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>OtherOther</td>
</tr>
<tr>
<td>Gerdie</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Jeffery Jardot</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>JobBoardsJobBoards</td>
</tr>
<tr>
<td>Joseph Stutz</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Joseph Freeman</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>JobBoardsJobBoards</td>
</tr>
<tr>
<td>Karen Jennings</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>JobBoardsJobBoards</td>
</tr>
<tr>
<td>Kevin Carlese</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Lanei Vasquez</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>GCCareerWebsite</td>
</tr>
<tr>
<td>Michael Rhoda</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Michelle Burns</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td>Polly Hays</td>
<td>[LinkedIn (LinkedIn)]</td>
<td>No</td>
<td></td>
<td>Internet</td>
</tr>
</tbody>
</table>
Bloodhound
Developed by @_wald0, @CptJesus, and @harmj0y.

Clean up that steaming pile of privileged users and ACLs.

Leon Jaimes [leon@sollievoit.com]
Bloodhound