Classified Data Hosting

Table of Contents

CREATED BY

LIFELINE™
DATA CENTERS

SECURE • COMPLIANT • SIMPLE

Executive Summary

Classified Hosting refers to maintaining critical and secret data that must still be used on a regular basis to perform business functions that are required for new/ongoing products or transactions. This secret information can be related to government work, like military production for DoD. Or, the information can be strictly in the private sector and related to something like R&D inventions or M&A activity which is regulated by the SEC.

In any case, secret data has become real in nearly all businesses and it is becoming increasingly regulated by the US Government and effectively regulated by the legal system. Auditors are being instructed to seriously look at security shortfalls and begin putting US companies on notice to remediate the security issues, or they will lose contractual agreements, or be sued in open court, all of which often amount to significant revenue.

Companies that have classified hosting requirements are generally very well run and contain many smart and agile people. These companies have made the focus of their business align with what they specialize in doing and have subsequently become a strong industry leader in those areas.

Many companies today are struggling to maintain classified hosting controls (for DoD work, or other internal needs) due to labor shortage and the fact it is an area that has grown in complexity and is not an internal business focus. Regulations, contractual agreements and litigation threat are mandating an update to the classified hosting methodology to comply with ICD 705, ICD 503, DCID 6-3 and CNSSI 1253. This will eventually be an absolute requirement by DoD, or it will become a practical necessity in order to avoid costly litigation.

Updating to these modern standards make US companies much more capable to obtain new opportunities and be able to quickly scale to the needs of future contracts and other business needs. By failing to maintain adequate classified control compliance, US companies are jeopardizing, or at least unnecessarily complicating their relationships withthe Accrediting Officers (AO) overseeing their data classification.

Lifeline Data Centers (LLDC) is expert at security controls and compliance. LLDC knows exactly how to work with the AO’s in developing ICD 705, ICD 503, DCID 6-3 and CNSSI 1253 compliance.

Working together with LLDC companies can meet all classified hosting compliance goals (current and future goals) economically.

Partnering with LLDC will:

- Free management to focus on tasks and strategies that move the company forward and acquire new business
- Bring companies into compliance with AO’s and auditors
- Allow companies to have fast scalability in reacting to new business opportunities
- Meet compliance regulations that are known to be on the horizon

Overview

This document has been created as a starting point for explaining and discussing outsourcing certain layers of a company's classified hosting stack. It would be LLDC's intent to eventually deliver a formal proposal after several design, planning and functionality discussions with corporate security and IT.

LLDC has significant experience in the following areas related to this type of project:

1) Developing secure hosting environments
2) SCIF design and construction
3) Working with authorizing government employees
4) Maintaining documentation required by US government agencies
5) Reporting security compliance to agencies monthly
6) Working through POA&M's

LLDC also a deep understanding of ICD 705, ICD 503, DCID 6-3 and CNSSI 1253 security standards and how those standards overlay NIST 800-53 R4. LLDC is FedRAMP, ISO 27001, PCI, and HITRUST complaint, as well.

Objective

Classified hosting is the practice of effectively implementing much tighter physical security, compute security, network security and user access security around a small segment of a specific data set.

LLDC understands that most companies maintain different classified hosting systems and all companies have different levels of security needs, based on data classification. These companies often experience several ongoing challenges, all surrounding the inability to have dedicated employees that can focus on the following issues:

1) Procuring and setting up new infrastructure dedicated to the classified hosting environment
2) Staying on top of software licensing expirations
3) Regularly (per weekly DISA notifications) applying patches to software and hardware
4) Correctly maintaining required evidence tracking and weekly/monthly reporting to DoD, or other agencies
5) Tracking ATO expiration and renewal dates
6) Maintaining proactive communications channels with AOs and auditors

Those issues create a barrier for the business units to quickly stand up new environments for new business opportunities and distract management from focusing on strategy and tasks that would move the company's agility and expertise forward, allowing the company to become more competitive in acquiring new business opportunities.

Companies must centralize all classified data to reduce overall cost of ownership and reduce data exfiltration risks. Also, companies must (by regulatory dictum) automate security, reporting, and incident response functions.

Data Classification

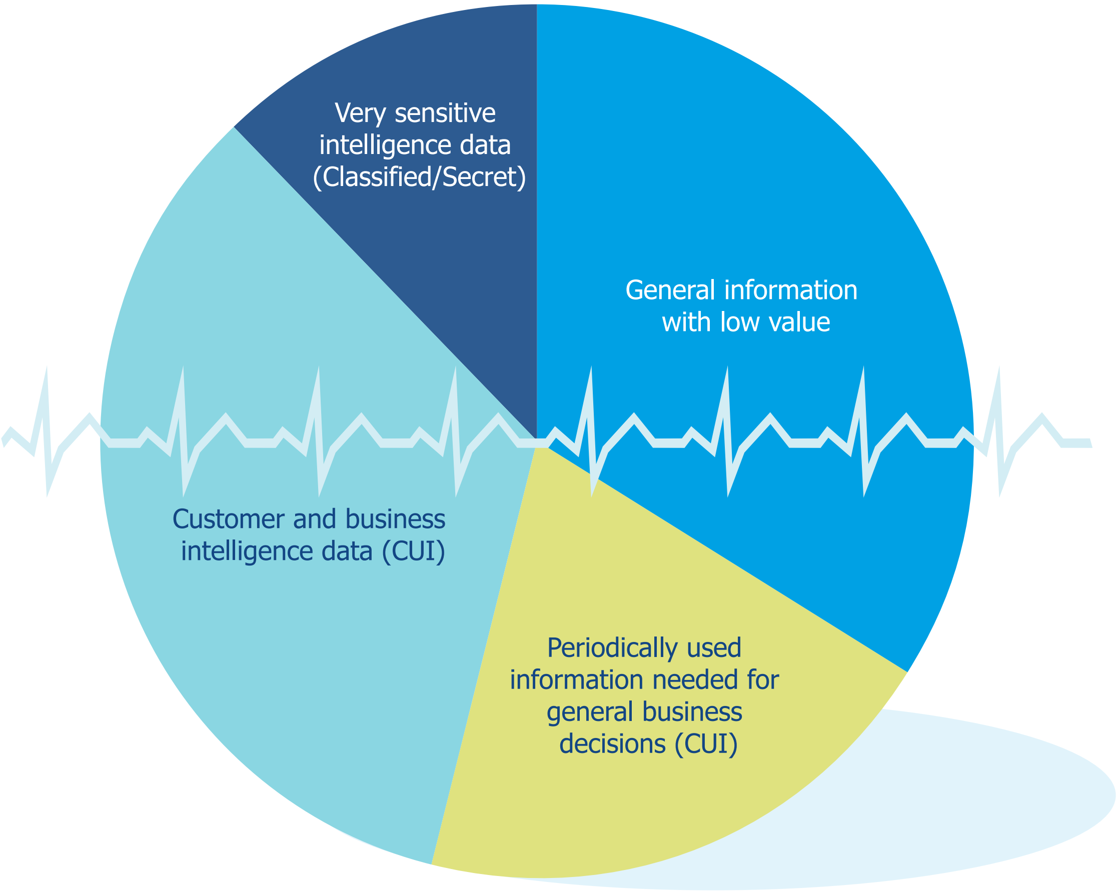
When an organization studies its internal data management and data classification needs, as a part of the Information Lifecycle Management (ILM) process, then data classification can be defined as a tool for categorization of data to enable/help organizations to effectively answer the following questions:

- What data types are available?
- Where is certain data located?
- What access levels should be implemented based on need?
- What protection level is implemented and does it adhere to compliance regulations?

When implemented, data classification provides a bridge between IT professionals and process or application owners. IT staff are informed about the data value and management (usually application owners) understands better where resources should be spent to maintain data security. This can be of particular importance in risk management, legal discovery, and compliance with government regulations. Data classification is typically a manual process; however, there are many tools from different vendors that can help gather information about the data.

Data classification needs to take into account the following:

- Regulatory requirements
- Strategic or proprietary worth
- Organization specific policies
- Ethical and privacy considerations
- Contractual agreements
- RBAC (Role-Based Access Control)



CUI = Controlled Unclassified Information

Solution

A series of meetings must be held in order to discover and document all Use Case Scenarios of the classified data that needs to be secured. The result of that discovery will validate, or modify the proposed system design.

LLDC then develops comprehensive plan and design requirements for a classified hosting environment that meets the company's current and future needs. The new environment will be scalable as needed by all business units that require access.

Project action items then performed by LLDC would be:

1) Working with agency AOs, auditors, and assessors to obtain their input and approval on a working set of operating controls

2) Obtain AO approval for new system design

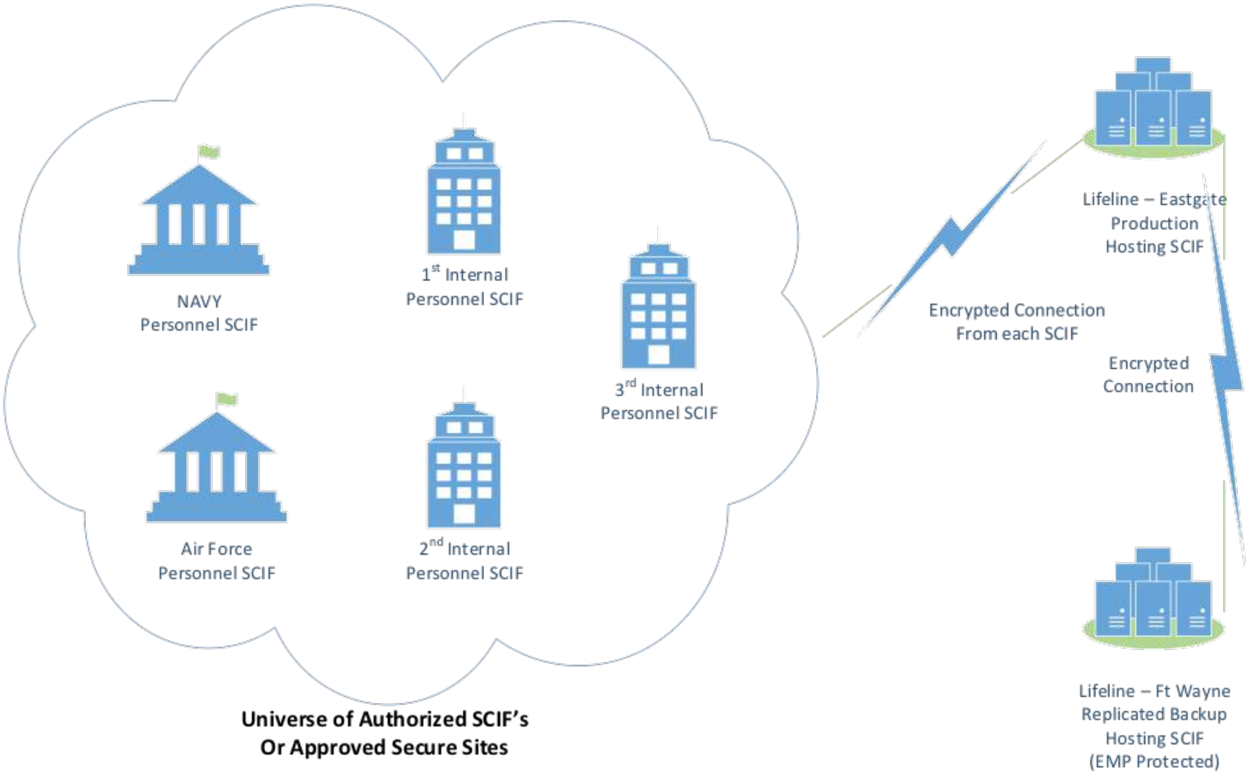
a) SCIF designs (SCIF Facility Checklist)

b) DISA IL-6 designs

c) Classified IT hosting environment designs

3) Build new classified hosting environment, including SCIF's and compute/storage/network equipment

Continued on next page >



Classified Hosting and SCIF Depiction

1. **Production and Backup Hosting SCIF would house a secure hosting environment and all data.**
2. **Any authorized SCIF with authorized, hardware, connectivity and knowledge would be able to work with the hosting system.**
3. **SCIF would communicate over DISA approved encrypted connections.**

4) Ensuring all required RR teams have appropriate access to the classified hosting system

5) Ensure all required RR employees have appropriate training to log in and efficiently use the new system

6) Frontline management for obtaining ATO's from agencies, or concerned data owners

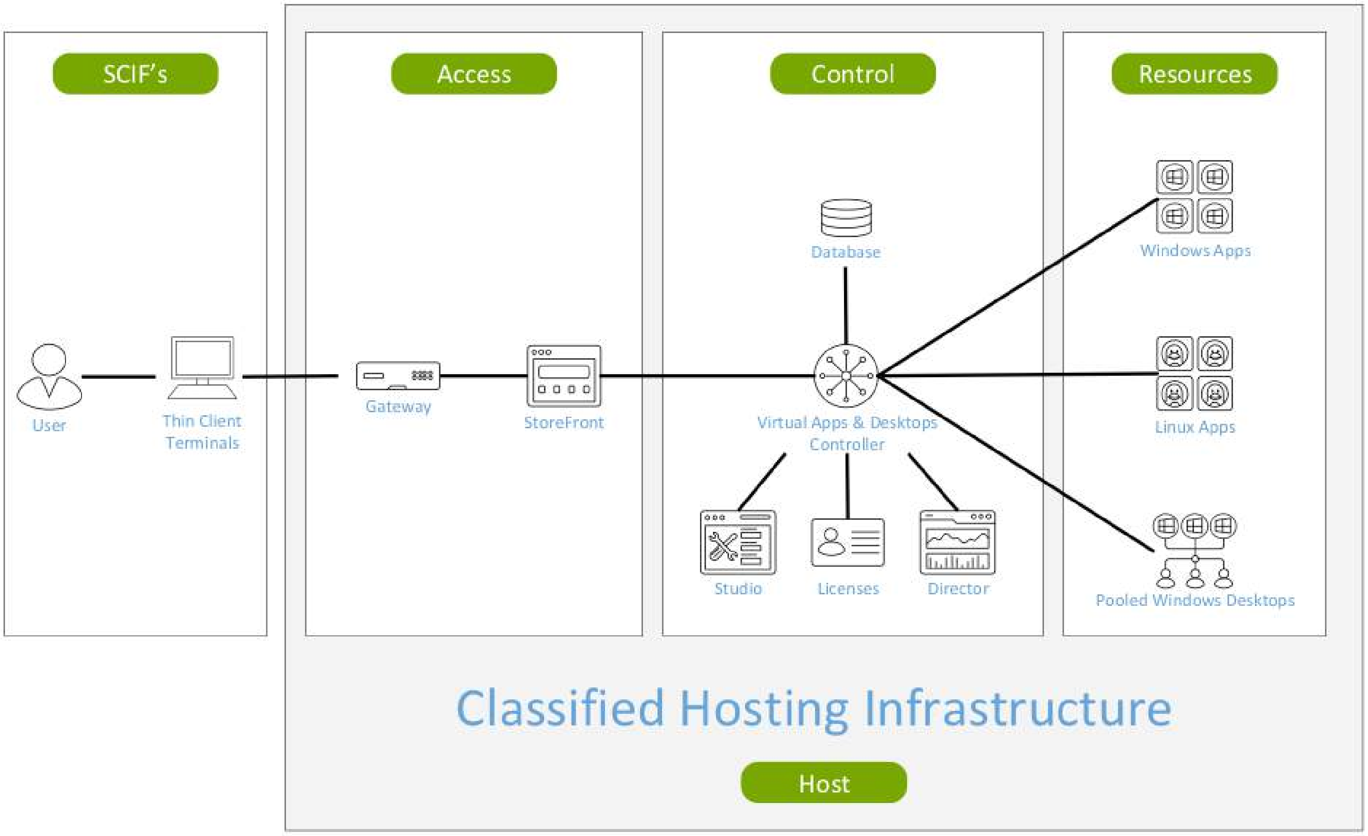
7) Begin cyclical reporting to AO's and modify those reports as requested by AO's

By creating new SCIF's that comply with ICD 705, ICD 503, DCID 6-3 and CNSSI 1253; then when one agency (or concerned data owner) approves an ATO it reciprocates to all other agencies by regulation and law. This significantly reduces costs and delays in future expansions and relieves the company from multiple reporting formats.

Lifeline will monitor the SCIF's and hosting equipment on a continuous basis. Lifeline will maintain all compliance data and perform the regular reporting functions to the appropriate agencies.

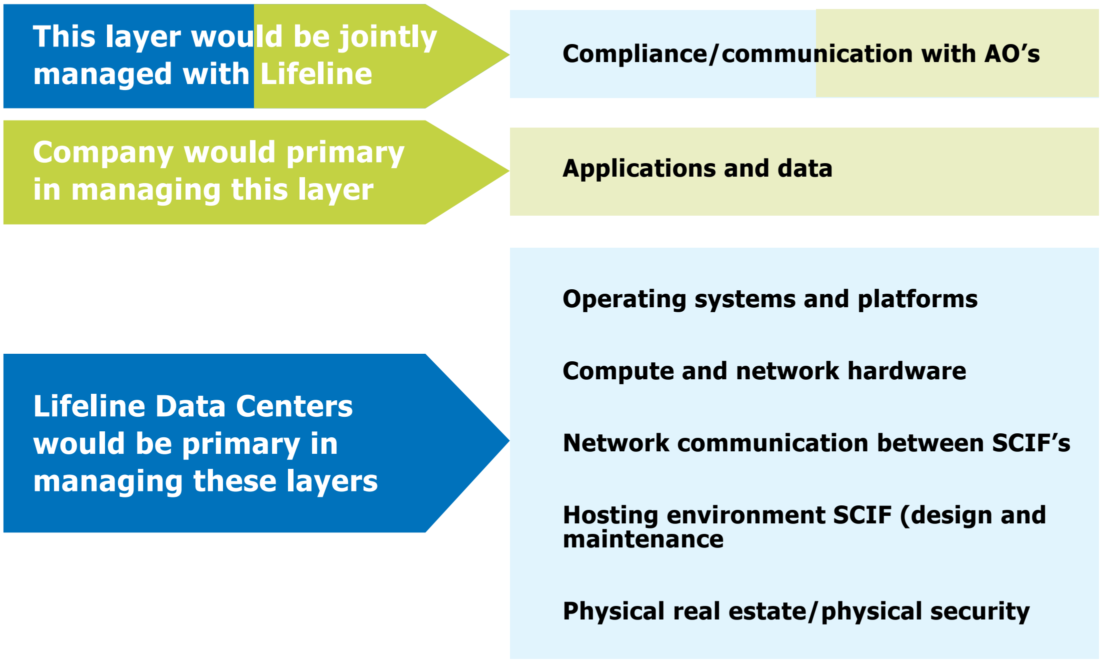
Lifeline and the company will meet monthly for a mandatory security and change control meeting.

Communicating from a Personnel SCIF, or secure area, to the Hosting SCIF will be accomplished over a DISA approved connection. The users will only access the hosting system through a thin client terminal.



Classified Data Hosting Stack

The following diagram represents different areas of roles and responsibility for LLDC and the classified data owner.



This layer would be jointly managed with Lifeline

Compliance/communication with AO's

Company would primary in managing this layer

Applications and data

Lifeline Data Centers would be primary in managing these layers

Operating systems and platforms

Compute and network hardware

Network communication between SCIF's

Hosting environment SCIF (design and maintenance

Physical real estate/physical security

LIFELINE™
DATA CENTERS
SECURE • COMPLIANT • SIMPLE

Contact:
Alex Carroll
(317) 590-0589 mobile
acarroll@lifelinedatacenters.com

Lifeline Data Centers provides outsourced, affordable data center facilities and services

Lifeline Data Centers is a leader in data center compliance, uptime, and innovation. Since 2001, Lifeline has provided data center and office real estate to companies who require uptime, connectivity, and room for growth.

- 99.995% uptime in n+n redundant facilities
- Compliant in all areas
- F5 tornado-resistant, redundant power and cooling
- Customized private cages and rack space
- Staging, storage and office space
- Underground hardened space
- Multiple carriers and no cross connect fees
- 24x7 NOC with managed services
- Primary data centers and disaster recovery centers
- Chicago colocation and Chicago disaster recovery alternatives
- Redundant Array of Generators™
- Redundant Array of UPS's™
- Redundant Array of Chiller Plants™
- Most Direct Power Path™
- Patented power and cooling delivery

We enhance our clients' position in their markets by eliminating the barriers to growth and change,improving operational efficiencies and reducing risks of managing complex information technology