

---

# HANFORD

# INFORMATION MANAGEMENT

# 2019-2022 STRATEGIC THEMES AND PLAN

*REV 1.0, 1/7/2019*

This document will serve as a strategic planning guide for a three-year window distilling a high-level approach down to a manageable perspective. The target audience is anyone who advances the information management (IM) aspect of the Hanford mission. IM leadership and technical staff will use this guide as a reference for decision making.

## VISION AND MISSION

### VISION

The vision of Hanford's IM program is:

To become more than a provider, we must be a trusted partner.

### MISSION

The mission of Hanford's IM program is to help people every day to do their work more efficiently, effectively, and safely through information, technology, and communications.

---

## SITUATIONAL ANALYSIS

The US Department of Energy (DOE) Environmental Management field offices in Richland, Washington are responsible for the Hanford site - the world's largest environmental remediation project as well as the largest nuclear construction project in the United States. Several prime contractors conduct work under the Richland Operations Office (RL) and the Office of River Protect (ORP). There is a single Government Owned Contractor Operated (GOCO) network/accreditation boundary with an Authorization to Operate (ATO). A second set of GOCOs/boundaries for the Waste Treatment Plant are in the planning/design stages.

## STRENGTHS

Due to IM's wise prioritization and investments, Hanford operates within a robust continuity of operations environment.

IM also has a strong, innovative engineering and integration staff, a proactive cyber program, and an appropriate focus on safety.

And finally, with a proven track record for delivering solutions on time, the IM program has management support, which is a critical component to its demonstrated success.

## CHALLENGES

Despite the IM program's strong ability to deliver, there are several challenge areas which will need to be overcome to continue to provide efficient, effective, and safe services. The most significant of these is an interrelated set of issues with broad ramifications which can be generally categorized under "Governance." Due to the multiple organizations with their separate management chains, a diverse set of contractors with unique contract scopes and differing individual missions, and a lack of formalized and defined enterprise architectures, IM governance at the site is limited. This results in duplicative investments with a snowballing effect on costs, data quality, and integration efforts.

As a result of decades of production and subsequent cleanup, a large amount of information exists within the networks' firewalls or as paper in boxes that could and likely should be available to the public. Much of this information is in systems utilized operationally. Making the information externally available requires enough investment that prioritizing it in the face of other investments with a tighter, more direct alignment with the mission is difficult.

Additional challenges are a lack of 'bench depth' (see Threats below), the push of budgetary efficiency having driven a shortage of overlap in many skill areas. This results in overwork of IM staff and sliding schedules when single staff members are absent. Related issues include the lack of readily available personnel in specialized or skill areas such as cryptography, identity management, enterprise software development, and user experience design. Addressing these issues will be challenging due to the government's inability to dictate personnel management

---

within the contractors. Appropriate work and deadline prioritization by all parties and well thought out budget justifications will help somewhat.

The “Internet of Things” (IoT) has acquisition and configuration management (CM) challenges – IoT devices are ubiquitous, inexpensive, and often not obvious (embedded functionality). Ensuring that the purchasing, tracking, and reporting of these devices are done according to proper procedures will be difficult. These risks can be somewhat mitigated with improved security techniques (automated inventory/scanning, heuristics). Additionally, IoT devices are renowned for security vulnerabilities – their very inexpensiveness means that manufacturers are financially discouraged from addressing existing devices as consumers are continuing to purchase them in droves. The typical personal IoT consumer doesn't necessarily know or care about the security risks of their IoT devices - they become someone else's problem (e.g. IoT botnet for DDOS). Just as with BYOD issues a few years ago, mitigation efforts focused directly at (specific) IoT vulnerabilities are not sustainable nor cost-effective. Instead, Hanford IM will need to focus on foundational security architecture and defense-in-depth. The same techniques that assist with addressing acquisition and CM challenges are also effective here, with the addition of exfiltration and command-and-control detection. The opportunities for IoT deployments are as varied as the devices themselves - common areas to consider are in facility management, safety, and logistics.

The final primary hurdle the IM program faces is the bureaucratic overhead and significant regulatory inertia, where formal guidance is unable to keep up with the pace of industry developments. This is evidenced in such areas as a lack of federal mobile stipends and reticence to use Unmanned Aerial Vehicles, to name just a couple examples.

## OPPORTUNITIES AND TRENDS

A significant segment of the workforce now understands the benefits associated with individualized technology and not only is in a “pull” mode, but actively spreading that knowledge and understanding, modeling it for coworkers. This organic (viral) approach, while slower, requires fewer resources and results in a broader acceptance. It should be encouraged where possible. (Also, see IoT above)

The emigration of many service providers to cloud-based offerings will have impacts for the federal government even for those agencies and offices that choose not to use the cloud. The commoditization of IT and influx of XaaS<sup>1</sup> providers will allow IM to provide services more competitively and with greater agility. Key to taking advantage of this will be secure and nimble data and flexible integration – allowing the seamless migration from service to service on the back end while continuously increasing in capability.

The Hanford IM program has taken advantage of opportunities for shared infrastructure with other organizations, such as the City of Richland and the Benton and Franklin PUDs, to the

---

<sup>1</sup> “X” as a Service – Software, Infrastructure, Platform via “The Cloud”

---

benefit of all. These types of strategic partnerships will continue to be sought as they allow for a significant increase in how efficiently taxpayer resources are utilized.

Industry developments in data science (“Big Data”) provide an opportunity for the Hanford site to mine current systems for business intelligence and utilize that information to gain insights and strengthen planning and budgeting via modelling, simulation, and other analyses.

The Free and Open-Source Software (F/OSS) movement continues to flourish. Many civil sector organizations, including federal agencies, are taking advantage of this and have implemented systems with significantly reduced licensing costs and capabilities equal to or greater than commercial alternatives.

Another trend which will continue to develop is the progress in machine learning or Artificial Intelligence (AI). Advances in this area allow the force-multiplier effect of technology to push further into the realm of "accomplished by humans." Challenges for AI are currently a scarcity of skilled developers, a pre-convergence ecosystem of platforms and technologies, and a lack of general experience in the capabilities of AI. The opportunities of recent developments in machine learning are still being explored. A few examples of AI techniques which could benefit Hanford are in the form of interactive chatbots for customer service or guided elicitation and processes, computer vision, content curation, and adaptive monitoring, alerting, and control.

Yet another trend which will see more development and impacts over the next five years is in unmanned and autonomous vehicles (e.g. drones, one-to-many fleets). UAV drones are currently in the valley of disillusionment while piloted-but-still-autonomous vehicles in general are in a pre-peak of the inflated expectations dip.

Other opportunities and trends include:

- Network Virtualization – the advances in virtualization of typical infrastructure layers, such as firewalls and switches, will improve the flexibility of existing data centers.
- Massive IT purchasing power at the consumer level – today anyone with a credit-card can spin up an entire virtual data center. The expectation for a complete eradication of Shadow IT is no longer realistic.
- Improvements in UX<sup>2</sup> in the commercial sector are yielding a user-pull for similar experiences with the (GOTS/legacy) tools and applications they utilize.
- Containers – ‘vanilla’ virtualization won’t go away, however more enterprises will see the benefit to adding containerization to the mix of solutions. A challenge for certain enterprises (such as government) will be finding the sweet spot between Software Quality Assurance practices and DevOps – this doesn’t originate with containers, but is contributed to by such.

---

<sup>2</sup> User eXperience

- 
- Encryption – over the next few years, several proofs-of-concept (such as zk-SNARK) that provide limited capability to work with encrypted data – while still encrypted – will move into a nascent product offering stage.
  - VR/AR – virtual or augmented reality has made a fairly big splash recently and appears to be working on establishing a foothold in the non-gaming enterprise. For all general organizations – e.g. not only those focused on utilizing specific engineering-overlay features – VR/AR will offer training benefits such as better engagement and retention. It might also feasibly be an alternative accommodation for certain disabilities.
  - Boutique manufacturing – commoditization of production technologies, both hardware and software, has allowed more “high end” products to be created by smaller less-well-funded organizations. Several of these technologies are climbing out of the valley of disillusionment and are ready for prime-time adoption. For some organizations this means easier access to more customized tools or systems. For others it poses a supply chain risk similar in some ways to what we saw with the advent of BYOD. When it becomes “bring your own factory” (or software development shop/app store) how will the organization ensure safety and quality are accounted for?
  - Blockchain – the distributed ledger concept will usher in several changes in existing distributed trust networks. Areas such as waste tracking and smart contracts stand to benefit from the development of this technology.

## THREATS & OTHER RISKS

The threats facing the IM program at Hanford are not entirely unique. As with many other organizations Hanford faces declining budgets, advanced persistent threats (cyber security), and a workforce increasingly accustomed to bringing their own “whatever” – whether it be a device or a service (“there’s an app for that”).

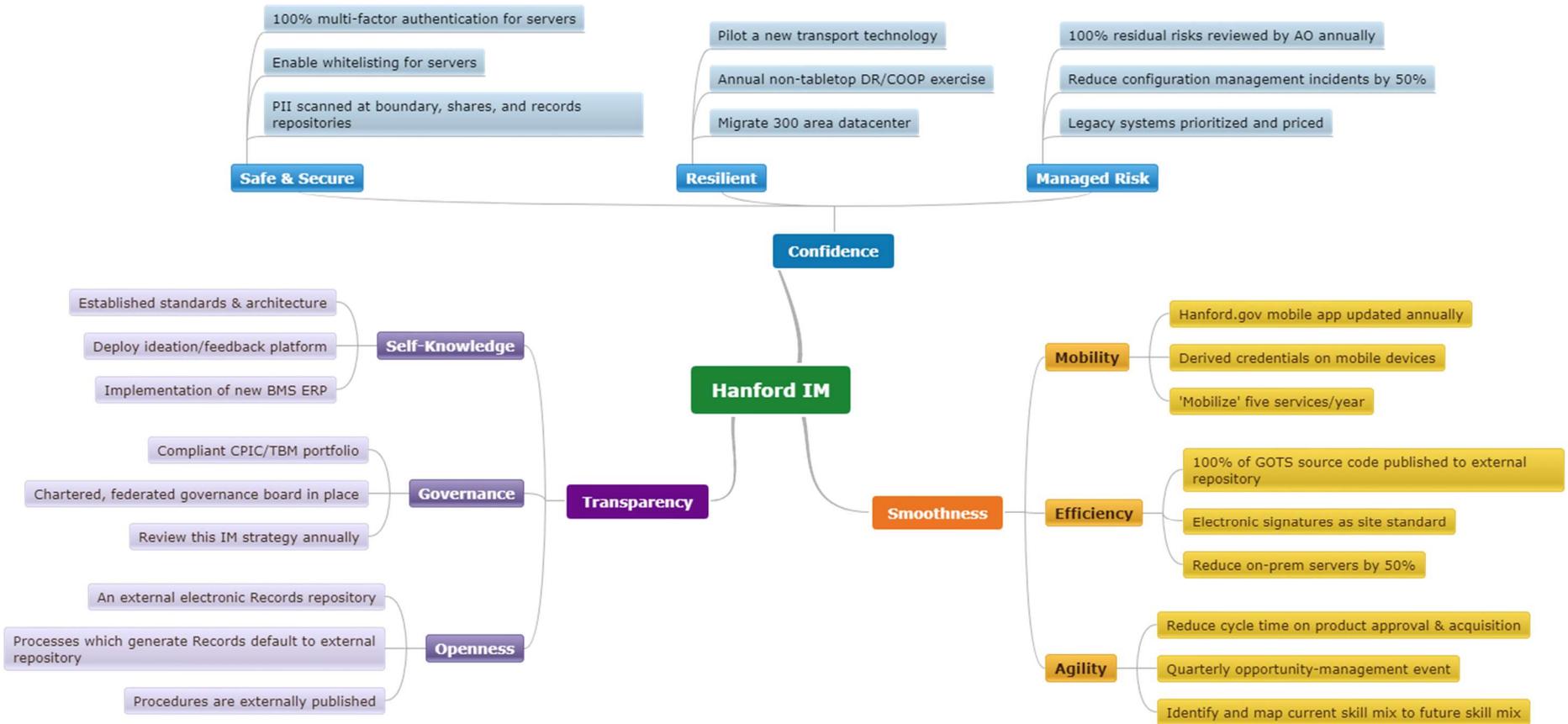
Additionally, the low number of local entities involved in information technology translates into a shallow pool of talent from which to draw. Federal and contractor organizations looking to find qualified personnel or those with skills outside general computer maintenance or network engineering must look farther abroad than the Tri-Cities.

---

## INFORMATION MANAGEMENT STRATEGIC THEMES

There are three interwoven high-level themes presented below (in no particular order of priority: Transparency, Smoothness, and Confidence), each of which represents an essential state-of-being for mission success. Each of these themes is further subdivided into three strategic outcomes, which are then supported by three tangible goals designed to be achievable within three years. Activities which align with one or more of these themes, outcomes, or achievements will create a foundation of building blocks for the future of the site. Most of these items support each other in an interrelated fashion.

This is not to be considered an exhaustive list of things needing work, merely the handful of areas which can be best leveraged for a significant benefit if given more concerted efforts. As these are mastered, reaching a sufficient level of maturity to maintain coherence when no longer a conscious focus, new themes, outcomes, and achievements will be woven into the strategy.



---

## TRANSPARENCY

### WHAT DO WE MEAN BY TRANSPARENCY, AND WHY IS IT IMPORTANT?

Transparency from the perspective of openness provides all parties visibility into decision making. It encourages accountability, participation, and collaboration while simultaneously reducing stovepipes and special interests. Another aspect of transparency is self-knowledge, as evidenced by a strong corrective action management program and quantitative management.

### SELF-KNOWLEDGE

**OUTCOMES:** The enterprise seeks to understand itself in a deep and quantitative fashion and utilizes that understanding to continuously improve by transforming data into information and subsequently into intelligence.

### **ACHIEVEMENTS:**

- **Established standards and roadmaps**  
Effective governance and configuration management requires a solid understanding of the current state. It is difficult to define a transformation to a target state without a known starting state. To help achieve the self-knowledge outcome, the enterprise must define and make known a set of standards and architectures. There should also be policies, roadmaps, and strategies related to the lifecycle of the standards and architecture.
- **Deploy ideation/feedback platform**  
An ideation platform provides the enterprise with a level of insight into culture and operational issues, fosters diversity and an environment where employees feel free to discuss topics without fear of retribution and taps into the distributed workforce expertise for new ideas.
- **Selection & implementation of new BMS ERP**  
The vast set of systems the enterprise relies upon for managing business operations is built upon a mish-mash of decades-old legacy applications. A new suite of elegantly integrated enterprise resource planning systems will provide better visibility and control of business processes and data.

---

## GOVERNANCE

**OUTCOME:** The enterprise has institutionalized processes and procedures to effectively and deliberately manage decision making around the use of IM budget as well as configuration management authority of the enterprise.

### **ACHIEVEMENTS:**

- **Portfolio is compliant with CPIC/TBM requirements**  
As the OMB requirements for full compliance with the Capital Planning Investment Control and Technology Business Management initiative advance, the enterprise must restructure the IM investment portfolio to not merely report but also manage to a sufficient level of granularity.
- **Chartered, federated governance board in place**  
As mentioned in the Challenges above, an organized governance structure will drive the enterprise to more efficient and effective operations.
- **Review this IM strategy annually**  
Due to the rapidly changing nature of information management it is essential that this strategic-to-tactical guide is reviewed on a frequent basis.

## OPENNESS

**OUTCOME:** All information, not specifically prohibited from public release by law, is available to the public in an easily consumable fashion.

### **ACHIEVEMENTS:**

- **An externally facing Records repository**  
A place where the enterprise can keep applicable electronic records in a fashion that is available to the public will increase efficiency, reduce costs, and promote trust.
- **Processes & procedures which generate Records default to the external repository**  
Once an external records repository is created, several gains can be had by creating policies and automating the destination for enterprise records which are not exempt from the Freedom of Information Act (FOIA). Furthermore, clearing<sup>3</sup> at the process level versus the individual products will yield a significant reduction in cost and workload.
- **Procedures are externally published**  
An external repository of non-OUO procedures promotes understanding and is a step toward establishing trust in the enterprise, especially when coupled with feedback and improvement loops.

---

<sup>3</sup> Clearing – the process of determining if information is exempt from FOIA

---

## SMOOTHNESS

### WHAT DO WE MEAN BY SMOOTHNESS AND WHY IS IT IMPORTANT?

The theme of smoothness is a fairly broad one. It conveys being unbroken, without difficulty or problem, tranquil, and polished. Additional contributory attributes of this theme are the concepts of friction and flexibility. Friction in this context isn't the physics sense of the word, but the representation of that boundary between the user and the systems and services they interact with. Too much friction diverts energy, increases stress, and diffuses focus. Conversely, too little friction may result in needless repetition or stalled processes. The organization should strive to manage friction to an appropriate level and increase the ease of use, simplicity, and elegance of the user experience and enterprise processes. Flexibility is the ability to gracefully bend, to adapt to changing circumstances. In the context of this theme, it is also being used to denote a reduced reliance upon fixed, monolithic architectures and an adoption of modular, extensible frameworks. Related efforts in this space have previously been referred to as "right-sizing" which means no more than ensuring the scale of the system(s) is only as large and complex as is necessary to accomplish the mission, and no larger.

### AGILITY

**OUTCOME:** The enterprise is well positioned to take advantage of opportunities.

#### **ACHIEVEMENTS:**

- **Reduce cycle time on product approval & acquisition**  
IM must work closely with other stakeholders, internal (information assurance, procurement) and external (vendors, headquarters) to the enterprise, to improve the time it takes to go from an identified need to an acquired product.
- **Quarterly opportunity-management event**  
Opportunity management is the flip-side of Risk Management. Six-Sigma/LEAN style events to discuss ideas (such as those generated by the ideation platform) and avenues to improve the enterprise and feed those into the opportunity register should be held on a routine basis.
- **Identify and map current skill mix to future skill mix**  
Opportunities will not always wait for the enterprise to be ready. A portion of the ability of the organization to capitalize on opportunities is whether employees with the appropriate skillsets are available. Proactively and strategically managing the workforce training, education, and qualifications will help with this.

---

## **EFFICIENCY**

**OUTCOME:** As the enterprise evolves, fewer resources are needed to achieve similar or greater results.

### **ACHIEVEMENTS:**

- **100% of GOTS source code published to external repository**  
In line with the initiative to push non-FOIA-exempt information outside, and the direction from both the White House and DOE OCIO, the software that tax-payer dollars have contributed to should be available to the public. Utilization of free/open-source code and a collaborative approach to development will result in lower costs and improved security.
- **Electronic signatures are site standard**  
Where signatures are actually necessary, digital signatures should be the primary mechanism. An increased adoption of automated forms and digital processes will reduce cycle times and improve records.
- **Reduce on-premise servers by 50%**  
A shift from government-owned servers to cloud-based systems (including “serverless” technologies) will improve organizational efficiency, reduce the IM footprint, and also improve the resiliency of the enterprise.

## **MOBILITY**

**OUTCOME:** Tools and information for enterprise users and the public are available on mobile devices.

### **ACHIEVEMENTS:**

- **Hanford.gov mobile app updated annually**  
The Hanford.gov mobile application(s) should be routinely reviewed for information assurance considerations and to ensure the information and services provided through the app are relevant and sufficient.
- **Derived credentials on mobile devices**  
Deploying a mechanism to push PKI<sup>4</sup> credentials derived from HSPD-12<sup>5</sup> identities on to mobile devices is the gateway to providing many more enterprise services to the workforce regardless of their location.
- **‘Mobilize’ 5 services per year**  
Having the mechanism to securely access services and information does no good if those services aren’t available. The enterprise should identify the five highest impact services per year and make them accessible on mobile devices, whether they’re government-issued or personally owned but government-managed.

---

<sup>4</sup> Public Key Infrastructure; cryptographic digital certificates

<sup>5</sup> Homeland Security Presidential Directive 12; smart-card badges

---

## CONFIDENCE

### WHAT DO WE MEAN BY CONFIDENCE AND WHY IS IT IMPORTANT?

Confidence in the context of this theme is used to mean assuredness and deliberateness, in addition to the traditional sense of confidence.

#### SAFE & SECURE

**OUTCOME:** The people and assets of the enterprise are protected.

#### **ACHIEVEMENTS:**

- **100% multi-factor authentication for servers**  
All servers, with no exceptions, must require a multi-factor authentication (MFA) mechanism to administer them. This may be “native” MFA such as smart-card logon, architecturally achieved by placing the servers behind MFA gateways, or some other mechanism.
- **Enable whitelisting for 100% of servers**  
All servers should enforce strict application execution whitelisting. This will reduce the risk of both malicious and mismanaged configuration incidents.
- **PII scanning at boundary, shares, and records repositories**  
The enterprise will continuously scan for personally identifiable information (PII) to ensure it is stored and managed in an appropriate fashion.

#### RESILIENT

**OUTCOME:** The enterprise has the ability to perform mission-critical functions with little to no disruption despite adverse circumstances.

#### **ACHIEVEMENTS:**

- **Pilot a new transport technology**  
Increased information flow across the site (and especially to the Central Plateau) is driving the need for redundant, high-speed connectivity. The current solutions are at or near capacity and must be refreshed with next-generation technologies – for example, broadband radio, 5G, and DWDM.
- **Annual non-tabletop DR/COOP exercise**  
Disaster Recovery (DR) and/or Continuity of Operations (COOP) exercises for IM should be conducted at a minimum of annually in a fashion that is more than merely a table-top discussion.
- **Migrate 300 area datacenter**  
The primary datacenter will be migrated out of the 300 area to a non-government facility, reducing the Hanford IM footprint.

---

## **MANAGED RISK**

**OUTCOME:** The enterprise is aware of the risk landscape, manages known risks, and seeks to identify and understand unknown risks.

### **ACHIEVEMENTS:**

- **100% of residual risks reviewed by AOs annually**  
Some risks previously accepted, including those accepted by former Authorizing Officials (AOs) may have changed risk profiles. The AOs should review all of the risks they are accepting on a routine basis.
- **Reduce configuration management incidents by 50%**  
Incidents arising from poor configuration management (CM) practices are a large source of problems. Focusing on better CM will improve the enterprise risk posture and improve efficiency.
- **Legacy systems prioritized and priced**  
A significant amount of effort and risk revolves around the large base of legacy systems at the Hanford site. The enterprise needs to ensure legacy systems are identified, mission and cost impacts associated with those systems and risks are priced, costs for system refresh are estimated, and these systems ranked in a priority order.