Cyber Security and Compliance Monitoring IT Compliance Inside the Federal Government

Bob Gourley
Chief Technology Officer
Crucial Point LLC

Please provide your comments on this presentation to:

bob@bobgourley.com

The Thesis of This Brief

- **During a period of dramatic change in IT and new emphasis on strategic cyber security, compliance monitoring and automated IT management are required.**

- **Lessons learned from industry dramatically reduces risk for successful implementation of compliance monitoring and automation solutions.**

Part One

A Time of Dramatic Change

The IT We Know Today Is Almost Over

Most Federal IT Today:

- Every organization has someone with CIO or CTO or J6/etc-6 title
- Customized, complex applications many designed locally
- Limitless user interfaces, each designed for customized, complex applications
- Proprietary datastores with business logic coded into the datastore
- Servers bought and owned by local IT departments
- Desktops bought and owned by local IT departments
- Desktops loaded and configured individually or by local IT folks
- Inefficient Datacenters
- Large Power Bills for Large Data Centers
- Fruitless attempts to satisfy needs of mobile users
- Knowledge workers who need automation but get poor IT service
- No understanding of the future of IT so no ability to plan
- Poor ability to search, poor ability to discover

How can we know what tomorrow's IT will look like?

- Track mega trends
- Track disruptive innovations
- Track what community leaders are doing
  - DISA, NSA, CIA, USDA, Intelink
  - Google
  - Amazon
  - Adobe
  - Sun
  - Cisco
  - New disruptors (like Endeca, Triumfant, Adobe)
- Technologies available today and trends moving them forward provide some very interesting conclusions relevant to all

Key Mega Trends for IT

- **Convergence and trend towards unified communications and user empowerment**
  - Consumerization is the most important component of this mega trend. All IT around the globe is being impacted by this trend. IT development will focus increasingly on consumers vice government or enterprises
  - Mass collaboration on problems. Social networking and IT tools to support that.
  - Huge increases in wireless/cellular bandwidth (10Gig wireless to desktop soon!)
- **Globalization and increasing internationalization of IT and demographic shifts**
  - US stockholders own most enterprise IT companies but most engineering is overseas (expect more enterprise IT solutions from overseas).
  - Decreasing Intellectual Capital Advantage of the US
  - Graying workforce in the US and other key Western nations (this trend impacts every ally)
  - Global competition for talent
  - This trend underscores the critical importance of coalition action and coordination/communication/collaboration
- **Increasing open development of software and hardware**
  - Embraced by all major IT companies and large numbers of programmers
  - This trend is fueling a growing need for in-house programming talent
- **Power, Cooling and Space (PCS) impacting data centers and every place computing is done**
- **Increasing pace of technology development and probability of disruption**
  - InfoTech, NanoTech and BioTech are building synergies off of each other
  - Must assimilate new technologies fast
  - Ugly fact: Our systems are in many ways subject to degradation, either due to malicious activity or due to interdependencies of complex systems

1) **These trends will impact us whether we like it or not.**
2) **All of these trends underscore importance of agility.**

Future of Information Technology

Virtualization

Sensor Feeds

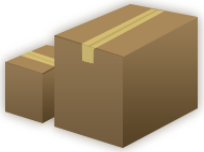
Robotics

Communications

Devices

Virtual Reality

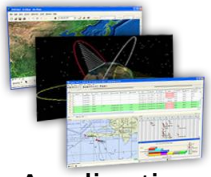
Visualization



Storage

Enterprise and
Grid Management

Operating Systems



Applications

Search

Collaboration

Security

Servers

What these many trends tell us

- Brace yourself. The relentless march of computational power and wireless connection speeds will bring more changes to your IT world than we have seen to date.
- Think of a flexible iPhone the size of a credit card with 10Gig per second connectivity. Think of that device connected to billions of sensors in buildings, streets, vehicles, clothing
- Think of this being viewed in easy to understand/comprehend ways (with Endeca-type guided navigation to all information)
- Software as a Service will accelerate
- Cloud computing (use of computations services from “the grid”) will accelerate
- Government IT powerhouses (like NSA, NGA, DIA, DISA, IMO) will deliver more and more capability to users via the grid
- Wireless comms to your personal phone and desktop will grow by an order of magnitude every two years

You should think through what your local technologists are doing
Why would any COCOM need a CIO?
What should J6’s do now? Do you need a J6? Or just a requirements person?

How Can We Accelerate The Future?

- Investigate new ways of encrypting data and identity management to enable better use of grid computing and to enable better use of commercial off the shelf devices.
- Speed the conversion of legacy applications and tightly coupled data to SOA-type model where data is separated from application.
- Investigate new ways to get devices, including desktops, that does not involve the acquisition executive needing to approve every purchase (if you can figure out how to do this let us all know).
- All IT departments move now to a terminal services model of desktop presentation.
- Establish new means to automate to reduce errors and costly downtime
- Ensure compliance with policy, especially security policy
- All IT professionals everywhere should learn and master ITIL. All those who develop SAAS should master CMMI.
- All leaders in government who do not know how to use IT should step aside and let others who are more qualified lead.
- Keep seeking out disruptive IT
- Maintain focus on user and the mission

The Comprehensive National Cyber Initiative

A Key Driver of the future of federal IT

- Will drive changes in automation
- Will drive changes in compliance of IT
- Will increase productivity
- Will increase security
- Will change the way we do business
- Will accelerate adoption of SCAP, FDCC, STIG

Part Two

Lessons Learned from Industry

Background

- Typically government seen as the source of regulation, not its subject
- Sarbanes-Oxley, Gramm-Leach-Bliley and Heath Insurance Portability and Accountability Acts are key examples of regulations impacting IT monitoring and compliance.
- Government IT professionals, who have always had demanding mission requirements, now finding they are subject to increasingly detailed regulation.
- Examples: Balanced scorecard approaches, FEA mandates, FISMA, Federal Desktop Core Configuration (FDCC), Security Technical Implementation Guides (STIG), Security Content Automation Protocol (SCAP)

Some Lessons Learned

- Reactive approaches to compliance are not reliable or scalable.
- Manual audits and manual manual follow-up are not efficient or effective and do not scale
- Annual audits are worthless and irrelevant and generally gundecked. Don’t do them, they are stupid.
- Automation is key, but automation should cover entire spectrum, from scanning to checking total state to alerting to remediation

Some Lessons Learned (Cont)

- Automation is required since simply scanning inundates IT staff
- Automating compliance by continuous monitoring ensures misconfigured devices are found immediately.
- Automating compliance reduces downtime
- Detecting, diagnosing and repairing changes before they become problems avoids work disruptions.
- Finding and fixing anomalies before they become problems keeps people productive and reduces manpower costs.

Some Lessons Learned (Cont)

- Automating audit reduces audit costs and makes audit results actionable
- Automation increases security. It is the misconfigured device that gets penetrated. Automatically detecting and reconfiguring out of compliance devices shuts the door to external attacks.
- It doesn’t make sense, financially or operationally, to be reactive in compliance. Every PC and sever can and should be monitored, and threats to compliance resolved every minute of every day. This enhances security and productivity and reduces cost.
- Key leader in this community: Triumfant. See http://triumfant.com

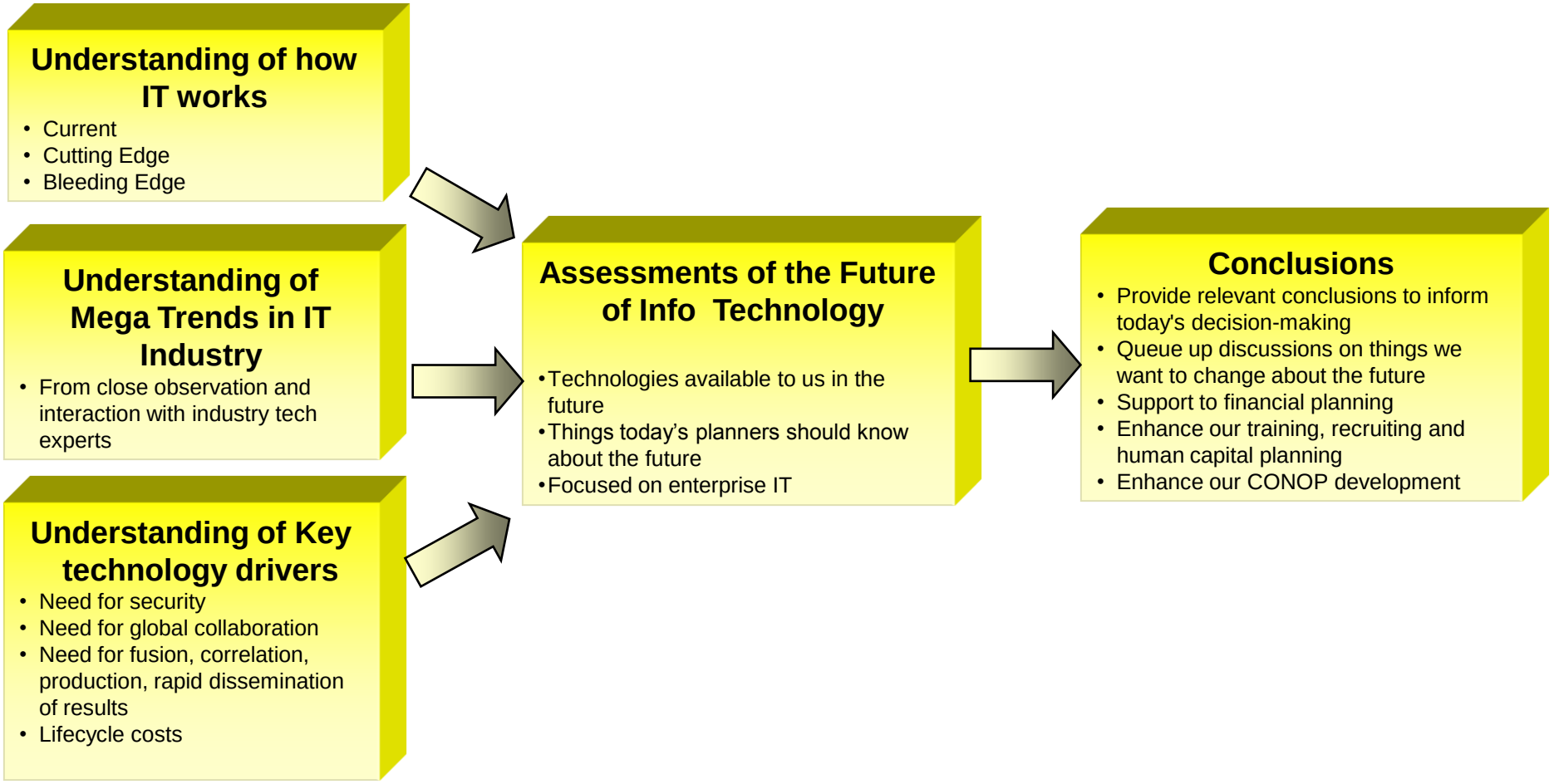
Concluding Thought

The sooner organizations in government implement an automated approach to IT compliance the better off we will all be.

Think SCAP, STIG, FDCC, Triumfant

Backup Slides

Methodologies



Sources of the assessments in this presentation include numerous Gartner reports/briefings, analysts with industry CTOs and other tech leaders, review of key online technical journals and interviews with technologists

Future of Information Technology

Virtualization

Sensor Feeds

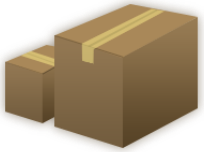
Robotics

Communications

Devices

Virtual Reality

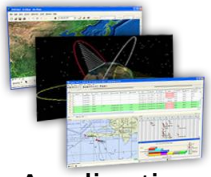
Visualization



Storage

Enterprise and
Grid Management

Operating Systems



Applications

Search

Collaboration

Security

Servers

Virtualization

- **Virtualization:** a technology aided technique for hiding the physical characteristics of computing resources, including making a single resource (like a server, operating system, application or storage device) act like multiple resources. It can also make multiple resources look like one.
- DTW (DoDIIS Trusted Workstation) solution is the most disruptive technology in DoDIIS today, and it is just one use one type of virtualization.
- Wireless laptops with totally virtualized, stateless power available today.
- Virtualization has proven effective as a means for increasing efficiencies, and as a potential solution for disaster recovery.
- Virtualization technologies will change the way agencies support all users, but most users will not know that.
- Virtualization is a flattener for hardware producers, which might change the hardware end of the PC and Server business. It will also likely impact our SOA with virtualized SOA environments.
- Over the planning period, Microsoft Virtualization will work best with Microsoft systems, SUN virtualization will work best with UNIX solutions, and VMware will be a strong player in both the server and workstation Virtualization markets.
- Products like Egenera for datacetner virtualization will be potentially revolutionary - Processing Area Network (PAN) architecture enables datacenter virtualization. The PAN combines diskless, stateless blade servers with a high-speed switch fabric and virtualization software that can dynamically allocate servers to applications on demand. Cassatt is another to watch.

The IC needs to leverage virtualization to better enable the secure insertion of COTS

Security Technologies

- **<u>Security Technologies</u>:** Technologies that contribute to the confidentiality, integrity and availability of information. Security technologies all operate under the configuration control and guidance of the Chief Information Assurance Officer. These technologies include: firewalls, intrusion detection devices, PKI, auditing, security testing, policy servers, and access control mechanisms.

- We are tracking the ability of government provided encryption to scale to future comms requirements.

- All IT providers are getting more serious about security, however, not one controls the entire stack, leaving lots of room for fault lines that can be exploited in standard commercial security.

- Identity and authentication of users will long remain a critical component of our security technology.

    - We do not expect any “Single Sign On” solution to provide comprehensive access to dispersed data. It will provide access to more and more data, but current data management/ownership constructs will prevent ubiquity.

- Cross domain solutions will all be governed at the enterprise-level. Individual programs will not develop their own cross-domain solutions.

Collaboration Technologies

- **Collaboration Technology**: a technology which assists humans in working together. In the this context, this is normally humans (probably geographically dispersed) working together to create intelligence.
- The age of stand alone collaborative tools (like IWS) is nearly over. Expect all future tools to be “collaborative” tools.
- Trends toward convergence indicate future collaborative capabilities will be centered on our existing full service directories and will also integrate standard enterprise scheduling software and DVTC and VOIP.
- IC analysts need means to collaborate via multiple paths at all levels. Pervasive tele-collaboration is a key requirement.
- Other key drivers will be the rapidly shifting consumer focused capabilities found in an increasing number of social software and other Web2.0 sites.
- This is not only about collaboration with intelligence but with customers. And it is most definitely about collaboration with allies.

Collaboration (continued)
The rise of Web2.0

Web2.0: Originally coined to mean the next generation net, its popular usage now has the term meaning "whatever is hottest/newest/available now on the net." The mindmap to the right is a now common concept for web2.0 constructed by Markus Angermeier.

Web 2.0 websites typically include some of the following features/techniques:

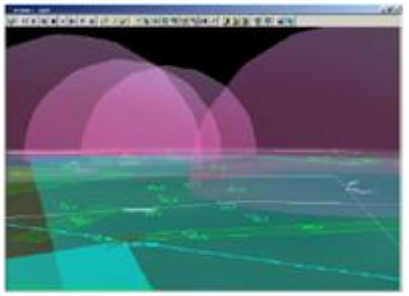
- Rich Internet application techniques, often Ajax-based
- semantically valid XHTML and HTML markup
- Microformats extending pages with additional semantics
- Folksonomies (in the form of tags or tagclouds, for example)
- Cascading Style Sheets to aid in the separation of presentation and content
- REST and/or XML- and/or JSON-based APIs
- Syndication, aggregation and notification of data in RSS or Atom feeds
- Mashups, merging content from different sources, client- and server-side. One to watch: JackBe (leader in enterprise mashups)
- Weblog-publishing tools
- Wiki or forum software, etc., to support user-generated content

All the big IT firms are moving into the Web2.0 world, including:

Cisco
IBM
Sun
Microsoft
EMC
HP
Oracle

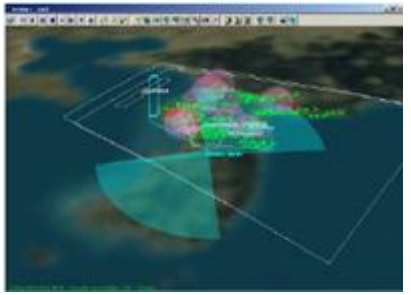
ISR Tools

- **ISR Tools:** In this context, these are capabilities that assist users in planning, visualizing, managing and directing collection over a battlefield.



- Too many of today's ISR tools are not fully integrated into the enterprise, resulting in sub-optimized performance for end users. Future tools are being written to take advantage of SOA concepts

- Expect more movement towards force-structure-aware networks



- Expect a greater ability to focus on long mission threads. And real time mission intelligence.

- Our newest, hardest missions require systems which can automate the population of knowledge bases, provide next-best observation, support uncertainty management, and provide integrated planning tools. Systems must enable real-time, dynamic re-tasking.

- SOA constructs will be the greatest single driver of future ISR tools, but in the context of ISR tools like DGCS, Web Services will NOT be the technology of choice for SOA. Too much data is being moved and too many users will need access to the tools and services for a web service approach to be used in SOA.

Service Oriented Architecture

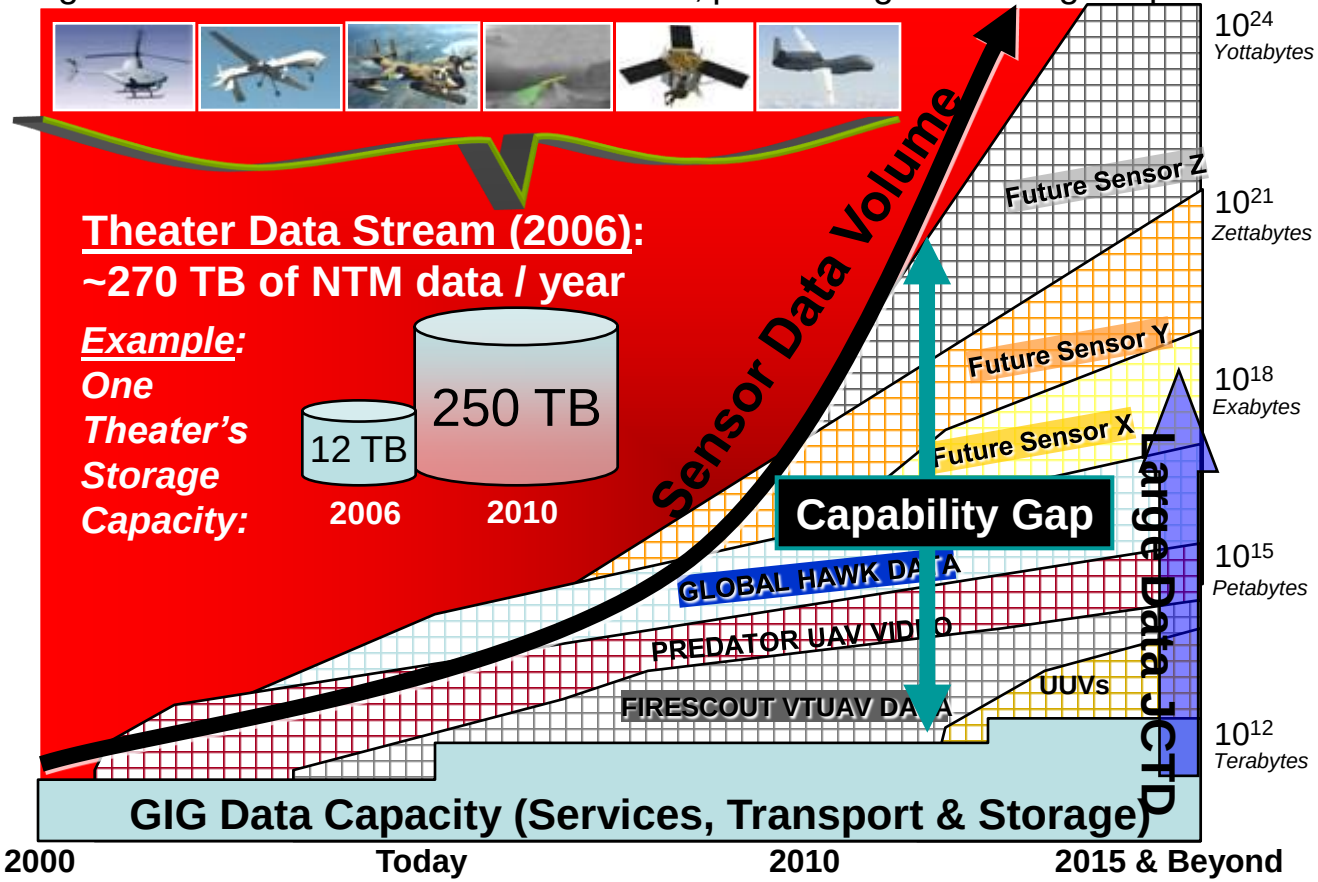
- **Service Oriented Architecture:** SOA is a design for linking computational resources (principally, applications and data) on demand to achieve the desired results for service consumers (which can be end users or other services).
- SOA will be an enduring design in the fabric. Goal is merging of loosely coupled components within a SOA.
- Offer user-configurable processes which can be changed based on need of the mission.
- SOA advancements will one day feed virtual reality modeling and simulation systems.
- One of the key goals of SOA design is agility.
- Expect SOA will continue to depend on smart integrations of key web service standards, including:
    - AJAX (Asynchronous Java and XML) – a technique for enhanced web based functionality.
    - SOAP (Simple Object Access Protocol) - For the start of web services communications
    - XML (eXtensible Markup Language)- For mark-up of all content
    - WSDL (Web Service Definition Language)- Defines how a service is described
    - UDDI (Universal Description Discovery and Integration)- ID and locate services
    - RDF (Resource Description Framework)
    - OWL (Web Ontology Language)
    - Business process registry- ID services by mission

Visualization

- **Visualization:** In this context, this refers to the ability to link the two greatest processors in our grid, the computational power of our enterprise and the human brain.
- The tie to commercial technology so far has not provided a good way to enable our analysts with wrap-around desktop screens. We meet needs by lining up more monitors next to each other. This clunky setup is pretty much the state of the art.
- But enhanced 2D/3D workstations with agile wideband interfaces to the brain are the need.
- Utility of capabilities like Touch Table or Jeff Han's Perceptive Pixel to visualize and interact with data shows promise. If live data is brought in these will be disruptive technologies.
- CAVE might provide another disruptive capability. Its use in multiple academic centers of excellence and its use in a couple of government locations is a positive note.
- SuperHDTV, HR Motion Imagery, 40Kx40K hyperspectral are driving key visualization requirements.

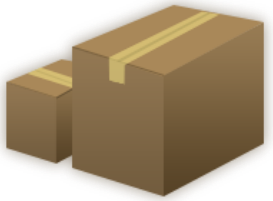
Sensor Feeds

- **Sensor Feeds:** The tighter linkages between intel and the operational DCGS/ISR capability providers is making the technology of sensors critical to plan for our future. Increases in sensor feeds are directly fueling our future needs for communications, processing and storage capabilities.



- **This chart captures some challenges in sensor feeds. They will grow faster than storage or comms. We must work with the ISR community to decide what gets kept and what gets stored.**
- **Will TPPU work in this environment? Do we go back to TPED?**

Storage



- **Storage:** In this context, we mean the ability of the enterprise to securely hold information. Our enterprise approach to storage is moving us away from storage tightly coupled to individual programs/projects towards storage that is managed as an enterprise mission/function.

- Enterprise storage options remain DAS, NAS, SAN with SCSI and iSCSI options. iSCSI will grow in the enterprise (different value propositions guarantee the continued coexistence of these options). All will drop in price and increase in capability.

- Rapid increase in sensor feeds will outpace our ability to store.

- Disparate, heterogeneous storage will be the norm well into the future. Distributed data synch and the software to manage data as an enterprise is the key requirement. Simultaneous shared access to large file storage systems. Data encryption at rest. More meta than data.

- Growth to multi-petabyte online distributed, federated archives. High performance grid storage. Massive Arrays of Idle Disks (MAID)

- Int ross the WAN (Infiniband?)

Terabyte (1024 Gigabyte)
1 Terabyte: 50,000 trees made into paper and printed
2 Terabytes: An academic research library
10 Terabytes: Printed collection of US Library of Congress
100 Terabytes: The entire internet

Petabyte (1024 Terabyte)
1 Petabyte: 3 years of EOS data
10 Petabytes: All US academic research libraries
100 Petabytes: All printed material

Exabyte (1024 Petabyte)
1 Exabytes: All words ever spoken by human beings

Zettabyte (1024 Exabyte)

Yottabyte (1024 Zettabyte)
1 Yottabyte: Everything that there is

Communications

- **<u>Communications</u>:** Most of which are IP based.
- SCI Comms between fixed facilities will be enhanced by a factor of 100 over the next 5 years.
    - We will need this enhanced capacity to enable true all source intelligence fusion
    - Enhanced comms is required for full support of virtualization and enterprise storage strategies.
    - Expect JWICS to transition to a HAIPE-based, IP infrastructure with an end-to-end pseudo-wire approach
- SCI Comms to most mobile users will always be unique.
    - Expect some use of technologies like WiMax for SCI over the battlefield
    - But the tactical environment cannot depend on the use of infrastructures required for commercial-like communications
    - The critically important demands of the tactical environment will always present challenges to dissemination of national intelligence to battlefield users.
- Infiniband is and open source based interconnect (likely the interconnect of choice for the future?). It is a high performance interface standard used to connect servers with remote storage, networking devices and other servers. Must also watch the DCE (Data Center Ethernet) interconnect standard.
- IPv6 is required, not just mandated. But stand by for new protocols that are more secure/capable.
- Comms must support real-time tele-presence and tele-collaboration.

Devices

- **Devices:** User hardware. The things applications and solutions run on. Workstation, Keyboard, Monitor, Mouse, Phone, etc.
  - Many completely stateless devices, but also traditional PC.
  - Expect continuing heterogeneity.
  - Integrated/converged VOIP/PC/Web service platforms.
  - Very high resolution geo-temporal displays.
  - Advanced video tele-collaboration.
  - New means of interacting with data (gesture).
  - Require advanced high res vis, wideband, agile human interfaces. Need good HMI on the front-end of everything (good use of both sight and sound).
  - Must load the human perceptive systems optimally.
  - Need low power, long life devices. Some wireless power.

Note: Kurzweil predicts that PCs will not exist by 2010. This is his way of saying stand by for massive disruption in this area–including info tech enabled biotech solutions for letting humans interact with processors

Servers

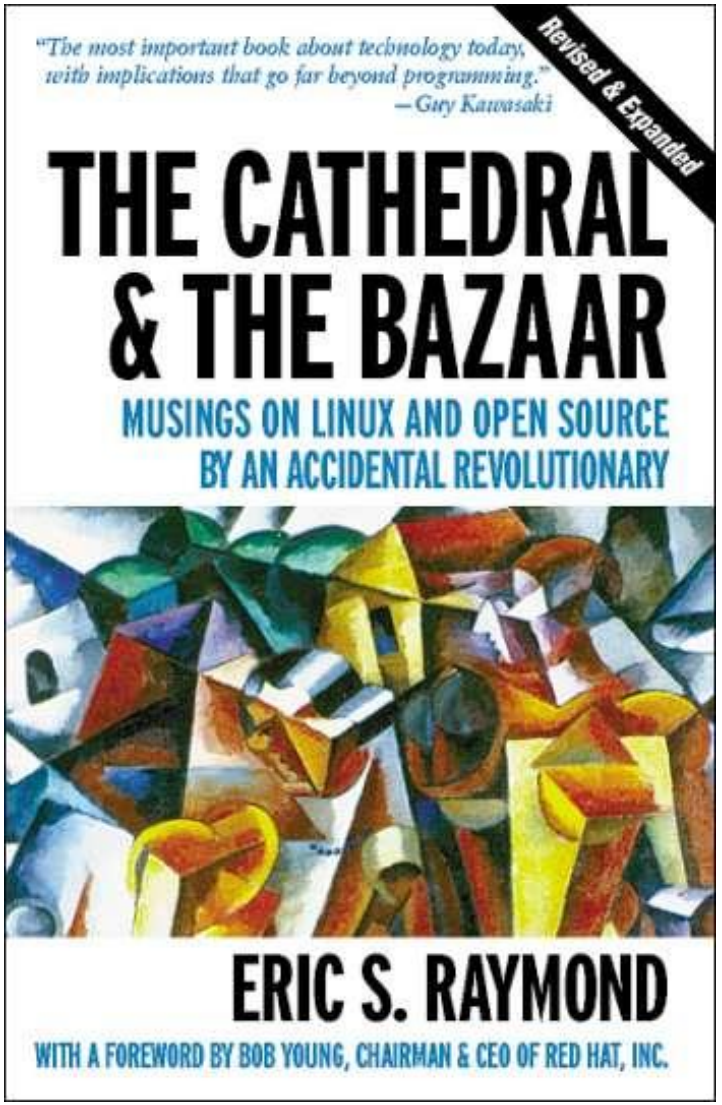
- **Servers:** Computers which host applications (and operating systems) for remote users.
  - Data centers are increasingly made up of disaggregated devices.
  - Blade growth will not accelerate.
  - Trend is for more comms direct to server core. We can buy off the shelf systems today with 20GigE direct to multiple core servers. Infiniband scales higher direct to core and across the enterprise fabric.
  - Everything becomes hot swappable in the next three years.
  - Moore's Law is not the best measure of computing performance. Core's law is alive. The number of cores per chip will double every 12 months.
  - Best measure of computing power is becoming compute power per watt.
  - Q: When could we replace a 10,000 square foot data center with a container? A: Today.

Information Access

- **Search:** In this context, we mean the computer based but human focused/driven examination designed to find that which is concealed. Search helps you find what you know exists and what you know you need.
- **Discovery:** Helps users find what they need, even if they don't know what to look for. This is a much more open ended problem. Gartner tracks both search and discovery in the category “information access.”
- Federated, semantic based search capabilities will continue to improve. But it is a flawed approach to think that an analyst must think of every possible question and search every database for every possible question. That does not scale.
- Expect continuing advances in new, more powerful search capabilities including in-stream media management using new multi-threaded capabilities. However, these powerful search capabilities are not keeping up with the drive to interconnect and access increasingly large data sets (which is required for horizontal interoperability). We will continue to face search-scaling problems.
- We expect richer, higher bandwidth interfaces into more human senses, including the use of more interactive interfaces. This is a movement away from entering terms into a web-based search box. First- the search box gets on every app, but later the search box goes away and is replaced with a statement of desire the computer always looks for.
- Federating and integrating results a long term challenge. Ensuring attacks on relevance also a challenge.
- Capabilities provided by leaders in “guided navigation” like Endeca provide disruptive capabilities we will want to accelerate into the environment.
- Architect so data finds data, the right info (and relevance) finds users, and users continually access relevance.

Open Source

- **Open Source:** This term refers to software that is developed with its source code open to review and input. Open source hardware architectures are also emerging a trend. Primarily uses open source protocols and procedures for our communications systems (the RFCs governing TCP/IP, for example).
    - Commercial and open-source solutions will increasingly be found in the same solution stack.
    - Open source software (including software you have no idea who wrote), will be part of every major solution.
        - There are some new risks here we will deal with
        - Issues can arise if there is sloppy (and inexcusable) practices of re-using open source without conducting any testing or characterization for suitability
        - Intellectual property indemnification issues
    - The biggest benefits to open source come from code sharing and reuse, as well as the ability to build on what is already there. Leveraging these benefits requires a framework for effective use of code.



Operating Systems

- **<u>Operating Systems</u>:** Software which ensures all computing devices can manage hardware and software. Orchestrate CPU, keyboard, monitor, mouse and other devices.

- Linux and Unix are predicted (by Gartner) to be on equal footing by 2010

- Linux and Windows have significant growth ahead, but a heated fight will probably present opportunities for Solaris

    - Partnership of Microsoft and Novell and recent dynamics between Oracle and Red Hat point to potential for rapid shifts in the Linux/Windows/Unix balance

- The long term future of Unix is not easy to predict at this stage. Today, it is the most powerful, secure OS in existence, and over the planning period it will remain so in DoDIIS.

- Given all the above, it probably sounds like a radical prediction to say that significant disruptions in OS's are not envisioned over the next 5 years. We will still see lots of Windows, Linux and Solaris.

Application Development

- **<u>Applications</u>:** Software that does stuff. Of most importance is the mission focused software of the enterprise. The primary point of user interaction.

- We will not have a single IDE or a single favored development tool/method/language. Expect .NET and J2EE battles long into the planning period. Also expect more LAMP and SAMP (LINUX or Solaris with Apache/MySQL/PERL/PHP/PYTHON)

- Expect stronger enterprise management of application development and more code reuse and service reuse. Also expect more efficient ways of transitioning code to operations.

- Services allowing users more power over their own app creation, including creation of composite apps (giving the ability to create applications to the people closest to the problem). Situational Software.

- Need apps and solutions that can empower users to get data/info their way and rapidly collaborate/create/share. Too few of today's apps do this well. Apps must access/leverage the Data Layer and fit in to the Service Oriented Architecture.

Robotics

- **Robots:** Electro-mechanical devices that can perform autonomous or pre-programmed tasks. Robots can operate under the control of humans, like the Predator UAV.
- Expect incredible increase in sensor feeds from UAV, UGV, USV and other robots
- Robotic sensors will place very high demand on our communications and computing infrastructures
- Storage of data and ability to search across it will also be impacted by the rise of robots.
- Collection management applications will need continual enhancement.

Virtual Reality

- **<u>Virtual Reality</u>:** In this context, this is technology that allows a user to interact with a computer-based simulated environment. The term encompasses modeling and simulation.

- New ways of modeling and simulation and collaboration will be created for our analysts and for our enterprise operators.

- Our workforce and our users, like other American IT workforces and users, is graying. Skills shortages will fuel an increasing automation of IT processes and user processes. This graying of the workforce will also drive simulation, modeling and prediction technologies– making this a major technology shift.

- Other uses of virtual reality will be found by our analysts and collectors.

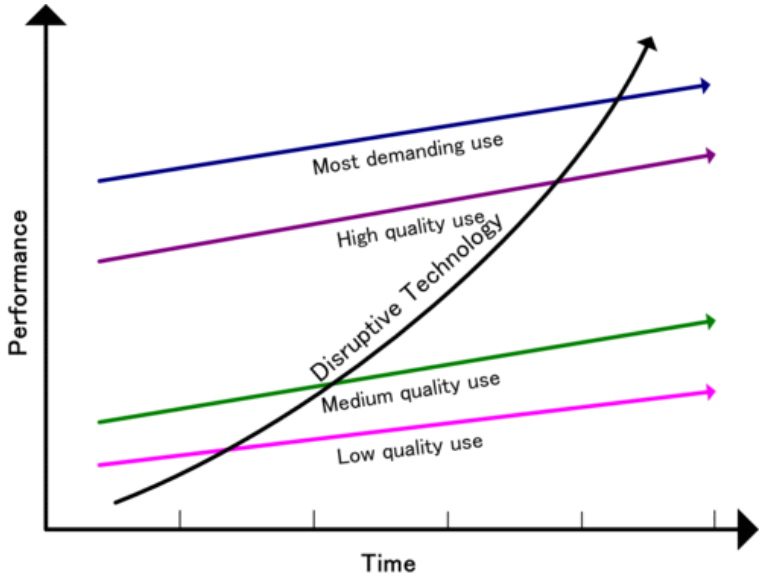
Enterprise and Grid Management

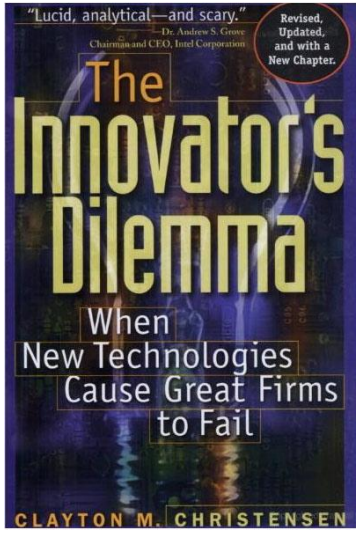
- **Enterprise and Grid Management:** In this context we mean the ability to lead and direct the entire enterprise, including the provisioning of compute power and the enterprise-wide virtualization, storage and communications capabilities.
- Increasing complexity of enterprises today means all technologists must have total visibility into the state of the enterprise and shared situational awareness.
- Do not expect comprehensive solutions to identity management and enterprise secure sign on within the next five years
- Goals for future must include self-healing enterprise capabilities.
- The Grid is only functional because of SOA approaches. Expect SOA approaches to continue for the near term.
- Related to **Utility Computing:** emerging technology used to provide resources on an "on-demand" basis
    - Dynamically allocates resources to maximize the efficiencies and minimize costs
    - Term "utility" is an analogy to other services, such as electric and water
        - Utility companies seek to meet fluctuating customer needs by providing resources "on-demand" and charging for services based on usage rather than a flat-rate basis
    - Also called "on-demand computing"

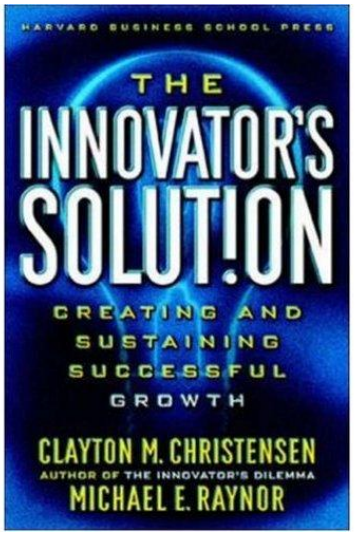
So What?!

- Real work and focused investment on the IT enterprise is positioning us to take advantage of new technologies– but we need to keep building on success and take steps for more agility in the enterprise.
- It is time to get in synch with if not ahead of the mega trends discussed in this presentation.
- IT planners are thinking and acting differently now.
- IT planners are being more proactive in defining what challenges are best resolved with tech solutions and which ones can be best addressed with policy or other changes or CONOPs.

Disruptive Innovation







A disruptive technology is an innovation that overturns the status quo in a market. The term was first coined by Clayton Christensen. He has also evolved the term a bit, now using "disruptive innovation" since more than technology is required to upset the status quo.

I continuously look for and list what I believe to be the most disruptive innovations for enterprise IT. For my list see http://ctovision.com

(Endeca is on that list)

This presentation…

- This presentation is meant to provide insights of use to today's IT planners. It is not meant to be about all technology. It focuses on technology for the IT enterprise.

- This presentation is not about the future of requirements, the future of policy or the future of CONOPs. But the future of IT is coupled to these subjects and some assumptions about those areas are made here.

- This presentation is still in draft form. It is being used to help dialog with other experts. If you are reading it your input is requested.

Today's Technologies

- Most IT now 20 to 30 years old:
  - RDBMS (Oracle, Sybase and other big databases are refreshed versions of 1970s technology)
  - Network-based comms (TCP/IP RFC written in 1973)
  - Mouse/keyboard/monitor interfaces (Engelbert patented Mouse in 1964)
  - E-mail
  - "Collaboration" through virtual rooms like JCE and IWS
- Some are only 10 to 15 years old:
  - Web browsers and web servers
  - Office automation tools
  - Business intelligence software
  - Many DoDIIS applications
  - Most computing and networking "standards"
- Some technology is newer:
  - Some enterprise management middleware
  - Some new collaborative and "social software" tools
  - Some new standards like JPEG2000 and OGC standards
  - Some new applications based on enterprise computing frameworks (.NET, J2EE).
  - Reusable services which can enable SOA approaches (including AJAX and Web2.0 approaches)

- **Much of what we use is based on old tech (that's not bad when the tech is still relevant).**
- **It can be really hard to bring a totally new thing into a large enterprise.**
- **We must find ways to bring things into the enterprise faster.**
- **And what we bring in might be here a long, long time.**

What the future tells us

- Plan now to enhance our agility. The most important agility is in our ability to analyze whether or not a proposed capability or new technology will actually result in a net gain in productivity and mission capability.
- Also of importance, but of a secondary importance to the above, we must enhance our ability to adopt new technologies. We must also speed our ability to configure existing technology. Some ways to focus on agility:
  - Find and eliminate applications/solutions that are not delivering required functionality or that can be terminated for other reasons. Do this to allow focus on newer, SOA type approaches.
  - Ensure our framework and integrators guide focus on agility
  - Find and eliminate unneeded work being asked of government or contract positions and refocus those positions on things that contribute to agility
  - Find more IC and DoD partners who we can team with to our customer's advantage (and find the right areas to divide IT challenges with). Drive for an IC-wide collaborative grid enabling all IC analysts, operators, collectors, leaders to interoperate and collaborate.
- Enhance our liaison and interactions with others, to enhance agility, to enhance support to customers on starved nets, and to avoid tech disruption. Interdependence will be an enduring requirement. We are in this together with our partners in and out of government.
  - Must enhance our tech liaison (and speed of tech exchanges) with allies.
  - For the government team, linkages to DISA are critical because of the challenges of disseminating intelligence to users in comms starved environments.
  - Nothing gleaned from a study of technology indicates any future challenges in partnerships with IC or other federal agencies or with Services or COCOMs.
  - The potential for disruptive technology from industry or academia (including DNA computing or quantum computing) is high during the planning period so liaison is critically important.
  - Fiscal realties will keep us pushing towards more common/economical solutions and better teaming agreements.

What the future tells us

- Keep appropriate focus and sense of urgency on cross domain. Collaboration with customers for analysis, production and dissemination will require well thought out cross-domain solutions that bridge different worlds.
- Refocus job skills to emphasize communications and enterprise storage management. Retain expertise in all enterprise IT technologies, but the mix of our technologists should shift to include more advanced network engineers and more enterprise storage technologists. These disciplines will become as important to us in the future as enterprise systems engineers are to us today.
    - There is a growing need for technologically savvy business process analysts who can create and manage and coordinate services for the SOA.
    - We also need more modeling and simulation process modelers who can build prototypes and predict the effects of new services and other enterprise activities.
- Build five year roadmap for our enterprise management toolkit and related enterprise visualization systems. All technology disciplines must have views into the state of the enterprise to ensure mission focus and agility.
    - The increase in virtualization and the increase in automation will make IT failure an even more costly proposition. This will drive the need for more complex enterprise modeling and simulation technologies.
- Plan now for increased engagement in the open source technology community. If we are using open source, widely known, multiple author software we should be involved in ensuring its quality.
- With growing concerns and government focus on environmental issues, expect increased adoption of “Green Technologies”

What the future tells us

- Plan now for redesign of JWICS to use new networking standards to ensure we are operating the grid at the highest possible capacity.
- Engineer for enhanced wide area wireless SCI capability. Which solution do we scale up? WiMAX?
- More IT workers will be user-facing. This parallels the trends captured by Gartner. Gartner predicts that by 2010, six out of 10 IT professionals will take on business-facing roles. Pure IT know-how will no longer be enough. IT workers will require strong leadership ability, knowledge of their non-IT partner mission needs, and knowledge of the processes of their customers.
    - Need more user-advocate-evangelists from IT into our users.
- Security will be a continuing concern. New techniques and tools are required to mitigate new threats, especially new threats regarding open source in our enterprise. Multi-level security and cross domain are enduring requirements.
- Automate with brutal efficiency

Pace of Technology Development

“Moore’s Law”	→	Computing doubles every 18 months
“Fiber Law”	→	Communication capacity doubles every 9 months
“Storage Law”	→	Storage doubles every 12 months
“Greg’s Law”	→	Number of cores on a chip doubles every 12 months
“Swatch’s Law”	→	Build it quick and get it out there and see if they like it