Monday

Connectivity as the Cornerstone of the Digital Revolution
Mr. Kevin McDermott
MuleSoft
1040 – 1125  River Rm 1

In this new digital era that we now live in, every digital innovation needs connectivity to make it viable. The more connections you make, the more value you get out of digital assets. Connectivity links your applications, data and devices with those of mission partners, suppliers, and even employees—to create a new breed of service offerings and capabilities. And given the number of applications, data sources and devices, the old way of doing this is just too heavy, costly and resource intensive.

Contrary to the popular myth, even if everything has an API, you still need integration. APIs facilitate integration, and integration platforms are key for fast API delivery. Join this session to learn how to leverage MuleSoft’s hybrid integration platform to create a connected enterprise that solves any integration challenge, whether SOA, SaaS or API oriented, in one centralized platform.

Cyber Range/Classroom Automation
Mr. Ken Oakeson
VMware Inc.
1040 – 1125  River Rm 4

The modern Cyber Range/Classroom is about the automation of the entire life cycle of an environment for production, dev, test, or classroom. Administrators should not be spending days creating the environment or cleaning it up. In this session, we will share the ability to:

• Standup a Cyber Range/Classroom in a repeatable manner that will ensure speed and accuracy without the complexities or management issues of bash or PowerShell scripting.
• How to create flexible building blocks that can be deployed with the click of a button
• We will focus on the importance of automating the standup of these building blocks
• Automated tear down of that environment when it’s not needed, to ensure resource availability
• End user portal access, with governance

Data Analytics
Mr. Derwin Warren
Cisco Systems
1040 – 1125  River Rm 6

The enterprise data center: a key element of any mission. It’s where mission assets and critical information is stored. As a result, it’s a prime target for advanced persistent threats (APTs), malware, distributed denial-of-service (DDoS) attacks, and insider threats. As data centers continue to get bigger and more complex, in addition to migration to public and DoD clouds, having visibility into the data center alone is not enough. You need to extend that visibility beyond into the base network. You need to be able to identify security threats and understand application behavior and dependencies in order to enforce security and policies consistently. Having visibility in this broad capacity is imperative when planning and managing segmentation policy and fighting today’s advanced threats. We will discuss integrated data analytics, application performance and network visibility platform based on machine learning and automated remediation.

Leveraging Cognitive Computing to Increase Readiness in the Digital Age
Ms. Alison Laporte-Oshiro
IBM
1040 – 1125  River Rm 5

IBM Watson Cognitive technology is being incorporated across various commercial industries and the use of cognitive technologies continues to expand. Now Watson is also delivering value to the automotive, aviation, and heavy equipment industries by optimizing maintenance, improving equipment and mission readiness and lowering operating cost.

In this session, we will explore how IBM’s Watson Cognitive Equipment Advisor has been piloted by the Army and will share the status, lessons learned and results that could be leveraged by the Air Force. The Stryker pilot was DoDs first use of cognitive technology to improve readiness of its vast fleets of aviation and ground equipment and the first-time sensor data has been used to bring a higher level
Industry Seminar Details

of precision to the maintenance process. This use case highlights how Cognitive computing can impact the maintenance/logistics communities to reduce cost and increase readiness for the many DoD and Air Force platforms.

**Internet of Things (IoT): Security Challenges and Its Impact to RMF and ATO**
Dr. Dean Albrecht
*IndraSoft, Inc.*
1040 – 1125 River Rm 3

RMF was introduced as part of NIST Special Publications 800-53 Rev4, 800-53A Rev4 and 800-37 Rev1. These documents provide guidance for enhanced security processes, a roadmap for migrating from DIACAP/DITSCAP accreditation, establishing security controls, and laying the foundation for continuous vulnerability scans. Automated enterprise network tools plus ancillary tools are providing accurate and timely operational results.

The next big challenge is Internet of Things (IoT) capability, which allows identification and tagging of discrete equipment and application components with an IP address. Challenges include implementation and configuration of IPv6, managing the IoT generated data (big data, data analytics), and implementing capabilities needed to manage IoT infrastructure, devices, and data. IoT capabilities can be very useful, but need to be vetted and secured—getting approval is not trivial. This session will provide insight into IoT challenges, identify potential impacts to RMF and ATO, and propose solutions for future planning.

**Why Digital Transformation through DevOps is Critical to Cyber Security**
Mr. David Roberts, Mr. Eduardo Krumholz
*Booz Allen Hamilton*
1040 – 1125 River Rm 7

Many of our critical DoD systems are vulnerable to ongoing cyber threats. These systems also suffer from software modernization challenges: Programs do not have the funds to simultaneously maintain current baselines, respond to security concerns, and modernize to provide additional value. Adopting a Digital Transformation approach based on DevOps techniques provides a path for programs to address cyber security concerns and modernize at the same time.

DevOps can have a significant impact on cyber security including speed, automation, and active detection. Speed enables quick fixes to cyber vulnerabilities, automated tools can be implemented enabling secure coding techniques and other DevOps techniques can help detect changes in software behavior and changes in system performance providing alerts to suspicious activities.

This presentation discusses how the following DevOps practices can lead to more secure systems: Configuration Management, Continuous Integration, Automated Testing, Infrastructure as Code, Continuous Delivery, Continuous Deployment, and Continuous Monitoring.

**Lessons Learned from DevOps Implementation**
Leidos
1040 – 1125 River Rm 2

To deliver operational effects and achieve information superiority, the Air Force needs to be embracers of innovation. The Air Force can achieve success by adopting an environment of collaboration between development and operations (DevOps) teams and technologies. Historically, the Air Force has maintained these groups as separate entities and relied on training and TTPs to bridge the gap. However the needed agility in the Air Force to deliver data at the speed of need has demanded a move to a continuous deployment approach.

Leidos offers lessons learned and thought leadership to deliver a tailored DevOps model for the Air Force. Our continuous deployment approach reduces operational risk and provides predictable and repeatable development and testing environments that accurately depict the operational environment. We offer a full spectrum view of the tools, tips, and tricks learned from over 10 years of supporting application developers, operations and sustainment staff and users. We infuse innovation in every step of the DevOps process. For example, we automate requirements collection and have made significant strides to self-provisioning. We also deliver the necessary documented and repeatable process for environment builds. We will demonstrate how our build process is repeatable and has
appropriate checkpoints to allow for stakeholders such as cybersecurity teams, operations and sustainment staff to review the environments to reduce final delivery. Finally, we automate release processes to allow applications to move from development, test to production in hours and days vice the current weeks and months.

Resiliency at the Edge
Mr. Jim Mann
HP
1040 – 1125  River Rm 8

In the Digital Age, cyber-threats continue to evolve to be more destructive and target lower levels of the compute stack. It is imperative that devices at the edge, those endpoint clients which represent an entry and exit point to networks, be designed with resiliency elements built-in, not bolted-on. Attackers who covertly gain a foothold on client end-point devices put your mission in jeopardy through “man in the middle” attacks, injecting malicious content or exfiltrating information. Attackers with denial of service goals who perpetrate destructive malware attacks can also put your mission at risk by creating extended periods of downtime. Recovery from such attacks, whether eradicating malware or reconstituting systems back to a state of integrity can be extremely difficult, potentially requiring a service event or physical replacement of impacted devices. In this presentation, you will learn about how full resiliency (protection, detection, recovery) can be accomplished in these devices, built on a foundation of hardware roots of trust which are resistant to even the most advanced persistent threats.

Adopting the Risk Management Framework (RMF) in Commercial Cloud
Dr. Benjamin Willett
Integrated Computer Solutions, Inc.
1135 – 1220  River Rm 6

A recent Presidential Executive Order has mandated that the NIST 800-53 security framework be used throughout the US Government. DoD has adapted NIST 800-53 into the Risk Management Framework (RMF). Come join us as we describe how ICS shepherded an Agile DoD program through the process of getting an RMF Authority to Operate (ATO) and also adopted and utilized RMF in commercial clouds.

or Managers: We will outline the process we used to obtain an RMF ATO for a DoD customer in under 90 days, managing to streamline tasks and optimizing the usage of subject-matter experts (SMEs). For Cyber Security Professionals: We will describe the security controls we addressed and the negotiations that occurred between our ISSM and AO.

For Software Developers: We’ll show how development integrates into RMF, what rules you must obey, and how to position yourself for compliance and easy audits, while improving your velocity.

Architecting to Increase Cyber Mission Effectiveness
Mr. Greg Mayfield
Gigamon
1135 – 1220  River Rm 5

Security Operations teams face greater challenges in combating data breaches. These challenges are due to insufficient time for threat inspection based on the ever-increasing speed of network data, as well as the vast number of attackers and resources available to breach traditional defenses and propagate undetected across most networks.

Traditional security models are increasingly ineffective and are hampered by limited visibility, extraordinary costs and reliance on manual processes to address incidents.

Gigamon’s Defender Lifecycle Model is an architecture designed to automate and accelerate the identification and mitigation of threats. Focused on a foundational layer of pervasive visibility and four key pillars — prevention, detection, prediction, and containment — the new model integrates machine learning, artificial intelligence (AI) and security workflow automation to shift control and advantage away from the attacker and back to the defender. Gigamon is the global market leader in Network Visibility Solutions.

Cognitive Security
Mr. Charles Fullwood
Force 3
1135 – 1220  River Rm 4
Cognitive security is defined as solutions that can understand context, behavior and meaning by analyzing both structured and unstructured security data. Cognitive security looks to unlock a new partnership between security analysts and their technology. These solutions can interpret and organize information and offer explanations of what it means, while offering a rationale for conclusions. In this session, we will discuss how Cognitive Security Solutions can:

- Enhance the capabilities of junior SOC analysts by giving them access to best practices and insight that used to require years of experience.
- Improve your response speed by applying external intelligence from blogs and other sources, so you can take action before signatures are available.
- Quickly identify threats and speed detection of risky user behavior, data exfiltration and malware infections using advanced analysis methods.
- Gain greater context around security incidents through automation of local and external data gathering and reasoning.

**Implementing an IT Management Proxy**
Mr. Jeff Hart
*M2 Technology, Inc.
1135 – 1220  River Rm 7

Maintaining information dominance in contested cyber theatres relies on secure IT command and control. IT management proxies were first deployed by financial institutions needing to expose IT services in support of Internet banking in the 1990’s and have since been implemented across the globe supporting financial, healthcare and government networks.

IT management proxies are commonly deployed to manage DMZs. A gateway appliance sits on the production network and a proxy appliance in the DMZ. All traffic is encrypted, whitelisted, blacklisted, inspected, reconstructed to remove possible malicious code, and share a single port through the DMZ firewall.

IT management proxies may also manage critical networks in the same enclave by placing management tools and proxy gateways in physically secure NOSCs. This allows ACL simplification replacing all ACL entries for management tools with just the proxy appliances’ ACLs.

**Journey to the Cloud: It’s NOT All or Nothing**
Mr. Tony Braddock
*Commvault*
1135 – 1220  River Rm 3

The journey to the cloud isn’t “all cloud or nothing”. With many datacenter solutions spanning multiple technological requirements, these environments can be physical locations being consolidated & moving to cloud as well as shifts for operating instances, workloads, applications, etc. Establishing “context” is a key consideration on the journey to cloud.

The benefits of cloud services (IaaS, PaaS, SaaS, etc.) can be significant for organizations but navigating through the needed considerations in determining workload applicability, cloud type (private, public, hybrid) is challenging especially if one needs to know exactly where the organization’s data resides, are proper controls in place, ease of retrieval in eDiscovery/OPRA scenarios, etc. Classifying one’s data portfolio is one of a number of preparatory steps needed to be considered to effectively use the right cloud service for the right use case. Other considerations include possible hypervisor transformation in moving workloads from on-prem to a cloud service for geographic business continuity purposes, ingress/egress costs of data & the benefits of having workload portability.

This session will help establish some foundational considerations needed to facilitate the journey to cloud and more quickly realize its benefits.

**Software Defined Everything: Integration of Satellite Communications (SATCOM) Networks and Gateways with Software Defined Ground Networks**
Mr. Bob Kimball
*Ciena Government Solutions Inc.*
1135 – 1220  River Rm 2

War fighting planners are increasingly concerned about operations in contested communications environments. The impact of contested satellite communications is particularly acute. Numerous planning organizations are investigating the possibility of agile failover from one satellite constellation to another and failover from Gateways in event of adversary challenges, including the use of commercial satellite resources. One of the challenges of this
approach is that to date, the terrestrial network is generally seen as fixed infrastructure without the ability to be modified in a timely manner to support fluid contested environments. Additionally, joint protocols and confusing rule sets to allow agile failover cause disagreement and indecision between Service and command users. This complicates and slows failover actions and C2. This project examines the capability of the union of dynamic software controlled terrestrial fiber networks with an agile satellite service management system. Overall system resiliency is increased by bringing more resources into the operational environment. This includes the possibility of failover of critical communications paths over different technologies; something not generally possible in today’s stove-piped environment.

**Operationalizing Threat Intelligence**
Mr. Rodney Butcher, Mr. Ryan Olson
*Palo Alto Networks*

**1135 – 1220**

River Rm 1

Effective network security must not only prevent known threats it must also leverage cyber threat intelligence to protect against unknown threats. Cyber threat intelligence itself must be collected from a wide range of sources & vectors, aggregated, curated, analyzed, and correlated, then rapidly deployed to enforcement points across the enterprise for automated & orchestrated action. Enforcement policy action themselves must occur across an increasingly heterogeneous environment from the network to endpoint to cloud. In this briefing, Palo Alto Networks will outline operational details of how IC/DoD/USG can leverage crowd-sourced threat intelligence from across the cyber security landscape, correlating threat sources, then using standards-based approaches like STIX/TAXXI to quickly distribute and implement protective measures.

**Training the Next Generation Cyber Warrior: An Emulated, Realistic and Risk-Free Cyber Battlespace**
Mr. Kevin Hofstra
*Metova CyberCENTS*

**1135 – 1220**

River Rm 8

As cyber professionals, we understand that in a domain as dynamic as cyberspace, our warfighters learn best through doing, rather than observing, which is why it is so critical that cyber operations training includes a hands-on mission rehearsal capability. Fortunately, the cyberspace domain provides a unique opportunity to create an emulated, realistic and risk-free environment for training, TTP development, experimentation and exercising. However, not all simulated cyber environments are equally capable of recreating the dynamic network protocols and events necessary to accurately reflect the indicators of compromise (IoCs) associated with the advanced persistent threats (APTs) representing the evolving adversary that our cyber warriors face. This discussion will cover the advanced techniques Metova uses to emulate the cyber battlespace of the future while seeking to reduce complexity through automation, reduce costs through open source & virtualization, and increase consistency/repeatability through lesson plans, exercises and scenarios. Finally, we will review two DoD examples of how Metova is using our Persistent Cyber Training Environment (PCTE) to train Air Force and Navy Cyber Mission Forces (CMF).

**Tuesday**

**Creating a Culture for Technological Innovation**
**Starts at the Top: Management Perspective**
Mr. Thomas Brazil
*Integrated Computer Solutions, Inc.*

**1030 – 1115**

River Rm 2

The challenges we face today, and the ones we will be facing in the coming years, are due to an exponential pace of technological change that is rapidly transforming our societies, competitive landscapes and impacting our defense posture. Despite the introduction of frameworks designed to aid organizations in becoming more innovative, there is still a pervasive reluctance at the management level to take the adequate and necessary risk to advance capabilities in conjunction with advancing technology. The danger of having this type of risk-averse attitude is the possibility of losing information superiority to the adversary. ICS has proven that building an organizational culture that enables technological innovation can be done without bearing the stigma of an implicit, unknowable risk profile. This presentation will provide insight to Management on intelligent vs. non-intelligent risk-taking in innovative environments - a distinction that should be
understood by Management and incorporated into your Innovation Process.

**Modern Active Directory (AD) Security for Today’s Enterprise**
Mr. Dan Conrad  
*One Identity (formerly Dell Security)*  
**1030 – 1115**  
River Rm 8  
Active Directory has been in a state of constant change in large enterprises since its inception. Within the Federal Government, a need for efficiency has caused many enterprises to reduce directories and merge to fewer and larger ones, expecting that fewer directories will be easier to manage and secure. However, many of these enterprises miss the opportunity to properly secure them and are full of “one off” exceptions to rules. As usual, the exceptions become the rules. The larger the enterprise the stronger the policies need to be. How can we grant the right permission to do the exact job?

In this brief we will discuss how and when to define the proper policies, how to have strong yet flexible delegation, and how to enforce the strong policies that you have put in writing across your cloud (Azure) AD and you’re on-prem AD.

**Exploring Successful Agile Transformation Patterns while Gaining PMO Support**
Mr. Steven Sanchez, Mr. Trey Henderson  
*Booz Allen Hamilton*  
**1030 – 1115**  
River Rm 7  
This presentation pairs emergent anti-patterns revealed during PMO agile transformation with corresponding adaptive practices aligned to a lean-agile mindset. “Starting with What You Have” may not be good enough to leverage existing performance based contracts and convince project managers that it’s ok (and expected) for cost and scope to be fixed while still welcoming change. In addition, the presentation explores the costs of delay when attempting to scale agile prematurely in PMOs.

Four agile lenses are presented to bring focus to decentralization, product ownership, capacity, and feedback/collaboration during the transformation while gaining support of often misunderstood roles such as program and project managers in a PMO. Adaptive practices discovered through these lenses facilitate more business ownership, promote PMO and partners as advisers, increase trust, collaboration, and product synchronization across PMO delivery teams resulting in delivering mission critical capabilities faster to warfighters.

**Rise of the Composable Enterprise**
Mr. Nial Darby  
*MuleSoft*  
**1030 – 1115**  
River Rm 1  
Today’s successful cyber organization crosses all boundaries and can quickly meet and adapt to mission requirements. Welcome to the Composable Enterprise. The composable enterprise casts away the hierarchical and hardwired systems and processes that defined its predecessors, and represents a rethinking of how technology can serve innovation and how innovation can serve mission requirements.

Organizations from any functional domain, regardless of how many legacy systems it has or how clunky its current processes are, can make the transition to a composable enterprise. To begin this journey enterprises can leverage modern APIs to create a flexible, agile network of building blocks representing their applications data, processes and devices. Developing this “application network” will deliver more than efficiency and lower-cost processing—it means heightened mission focus through digital engagement and analytic decision making. Through this presentation, learn what makes a composable enterprise and how to transform your organization and create an application network.

**Cyber Enabled Infrastructure**
Mr. Scottie Ray  
*VMware Inc.*  
**1030 – 1115**  
River Rm 4  
What if you could transform your organizations cyber-defense capability within your currently deployed infrastructure? Turning your existing datacenter infrastructure into a “sensor grid” that thwarts malicious behavior. The ubiquitous Virtual Infrastructure within your datacenter is enabled to act as a cyber-defense platform to detect, protect and respond against cyber-threats.

This cyber-defense capability exists in a unique place in the
datacenter that is close enough to gain detailed context into an application’s runtime environment but protected so as not to be compromised in the event of an attack. The Virtual Infrastructure performs this function by first establishing the authoritative intended state of an application, then monitoring that intended state for any deviation and if deviation is detected orchestrating an incident response. It includes the ability to detect anomalous behavior that would typically be unseen, to block malicious threats while they are being created, and to respond by automatically remapping the environment to contain threats.

This capability represents a next-generation approach to cyber-defense by taking a different approach to security by cyber-enabling existing, widely deployed, infrastructure as opposed to attempting to enhance security by bolting it on to existing infrastructure. It represents a significant cost savings by both leveraging technology currently in-place as well as preventing the need to expend significant operational cost by implementing a security solution that requires re-architecting the current infrastructure. The Cyber-Enabled infrastructure represents a programmable security layer that allows for cyber-security innovation moving organizations and the cyber workforce from a manual intervention model to an intelligent automated response based on next generation security policy.

Agile software development methodologies have grown in popularity since the publication of the Agile Manifesto in 2001. The manifesto advocates four principles of shifting emphasis: (1) individuals and interactions over process and tools; (2) working software over documentation; (3) customer collaboration over contract negotiations; and (4) responding to change over following plans. However, use in the DoD has been limited and met with varying degrees of success due to such factors as a tendency to require monolithic milestone deliveries based on acquisition processes, contractual compliance and organizational policies, and processes/procedures that are above the program level. These factors lead to questioning the validity of Agile processes. We will present our practical experience in implementing Agile software development across several Government contracts, elaborating on the core elements of Agile processes that we have applied within the constraints of the Government challenges. These elements are A-Accountability, C-Collaboration, C- Commitment, and T-Transparency.

**Blockchain: A Digital Age Transformation Platform for DoD**

Mr. Mark Fisk
IBM
1030 – 1115 River Rm 5

The capabilities of Blockchain are starting to impact US Government and DoD business networks. How can you get a better sense of what Blockchain is, how it will be leveraged by government and what is the technology behind it? Will you be participating in commercial blockchains, standing up a blockchain to solve a tactical problem, or bringing together a business network to consider transformation of a current business process leveraging blockchain to provide new value to all participants? This session will explore the basics of Blockchain, explain why a permissioned blockchain is the right answer for government, and investigate key use cases in pilot/production where the promise of blockchain capability is being realized today. IBM will also provide an overview of how to start with blockchain technology in order to allow your organization to prepare to leverage the trust, transparency, and accountability that blockchain can bring to your business network.

**The Evolving Threat Landscape – Current Trends in Threat Intelligence, Ransomware and Exploit Kits**

Mr. William Largent
Cisco Systems
1030 – 1115 River Rm 6

Cisco’s Threat Intelligence organization is the industry-leading threat intelligence organization dedicated to providing protection before, during, and after cybersecurity attacks. William will lead a discussion on the current and emergent threats, including ransomware, exploit kit activity, and current trends in the constantly evolving threat landscape.

**ACCT Agile**

Mr. Jeff Cecil, Mr. Raj Lingam
IndraSoft, Inc.
1030 – 1115 River Rm 3
Augmenting the Cyber Reality
Mr. Paul Krein
Red River
1125 – 1210
River Rm 5

Today’s Cyber landscape IS now today’s IT Landscape, and the traditional route where a majority of the cyber funding of the past was spent on developing a hard outer shell of defense mechanisms are far from sufficient. Talented Cyber security analysts and resources are becoming limited these days. The explosion of data – both the mission data, and infrastructure machine data are overwhelming conventional tools and analyst capacity. IT and Security executives are working together across many operational aspects seeking more effective ways to address the rapidly changing threat landscape.

In our talk Red River’s CTO will discuss how IT and Security teams alike are employing advanced processes, machine learning and new capabilities embedded through the network, systems, and organization to handle this onslaught of data. Mission and IT owners will discover how the new security posture and foresights available through integrating proactive and dynamic data loss prevention techniques, network and user behavioral analysis, and machine learning will augment and offload the human burden to search out and correlate potential threats and identify seemingly unrelated patterns.

We will explore how continuous improvement, learning from incidents, incorporating real-time telemetry, and analyzing retro-active playback can yield new insights to the policies and processes in the incident response plan with the goal of ultimately connecting the right users with the right data securely.

Agile Dynamics at Scale
Mr. Sean T. Ricks, Ms. Vivian L. Martin
MITRE FFRDC
1125 – 1210
River Rm 3

A key function of the Business and Enterprise Systems (BES) Directorate is the development or acquisition of new software to deliver innovative capabilities to support the warfighter. Several BES programs have considered the Scaled Agile Framework (SAFe) as a basis for their development processes. In order to improve the effectiveness of these processes, we have developed a system dynamics model that simulates the flow of work through a virtual SAFe program. This model can be used to experiment with different policy parameters such as sprint length, team size, and continuous integration effort to see how these parameters affect the rate at which work is completed. This model will form the basis of a management flight simulator that BES program managers can use as a decision support tool to determine which policies to implement in their own development programs.

Cyber Common Operating Picture
Mr. Jamie Miller
Mission Multiplier
1125 – 1210
River Rm 2

Achieving a cyber common operating picture (COP) is an innovative/cost effective solution to provide continuous monitoring and risk scoring, and to achieve real-time security monitoring of cyber threats and vulnerabilities. An effective cyber COP solution is founded upon mapping secure content automated protocol (SCAP) enumerations to select NIST 800-53 controls and custom cyber “key effectiveness measures”, and designing a control database/warehouse that interfaces with a dynamic executive dashboard that reports results based upon an agreed risk scoring logic. The capabilities of an effective cyber COP solution include the integration of “real-time/automated data feeds” into a database/warehouse and development of a risk scoring dashboard to assess risk across cyber domains, to include – vulnerability management, asset management (hardware/software), patch management, configuration management, event management, and malware management. The end result is that stakeholders have access to accurate, current, and actionable data (enterprise-wide) to make more informed and cost-effective risk management decisions.

Operating in the Cyber Domain: Shoot, Move, Communicate – projecting power and access while ensuring/protecting communications
BG (ret) Fred Henry
UNISYS
1125 – 1210
River Rm 7

Building highly secure, yet dynamic networks that can
Industry Seminar Details

continue to deliver the mission, even while compromised is now in the realm of possible. Modern day networks need to be able to incorporate security and extreme agility in order to meet the constantly changing security landscape enabling 100% secure communications, even for situations and/or threats that are still unknown. In addition, these dynamics need to be delivered, on-the-fly, anywhere at any time and at any place on the globe. The discussion will focus on concepts and methodologies that will enable organizations to achieve these objectives.

Analytics in the DoD and the Rise of User Self Service
Mr. David Sears
Tableau Software
1125 – 1210 River Rm 6

The Department of Defense has more data than ever before. Data has become as important to the Department of Defense as fuel is to an airplane. Yet, like enterprises everywhere, analysts struggle to organize it, decipher it, visualize it, and use it to make the best possible data driven decisions. The importance of a modern day Visual Analytics Platform is critical for the future success of the Air Force in maintaining data analysis superiority. Modern platforms reduce the limitations of the report factory. This presentation will review these data challenges, identify key areas of DoD analytics focus, and describe and show relevant customer examples for Department of Defense Use Cases.

Protecting the Increasingly Heterogeneous Enterprise
Mr. Rodney Butcher, Mr. Ryan Olson
Palo Alto Networks
1125 – 1210 River Rm 1

Large enterprises, from Government agencies to corporations, are increasingly distributing workloads across a heterogeneous environment comprised of networks (wired and wireless), endpoints (WinTel, Linux, Mac, Mobile, IoT), and clouds (public, private, hybrid). Securing the enterprise and the data on which it relies requires increased visibility into applications, users, and traffic flows, as well as up to date intelligence on threat actors. Enterprises must then be able to affect consistent security policies across network, endpoint and cloud in response to threat conditions. In this briefing, Palo Alto Networks will describe how large enterprises worldwide are leveraging an orchestrated platform-based approach to prevent cyber-attacks and strengthen the overall security resiliency of their organizations.

Public, Private, or Hybrid? Which cloud infrastructure is best suited for your Agency?
Mr. Greg O’Connell
NUTANIX
1125 – 1210 River Rm 4

The Federal Data Center Consolidation Initiative (FDCCI) and Cloud-First mandates have driven Federal agencies to shift the way they have operated and managed their IT infrastructure. Government organizations demand the benefits of public cloud, including the promise of cost savings, agility and scalability, but many agencies often find costs are higher than anticipated along with challenging technical issues.

In April 2017, Nutanix commissioned a study on government cloud usage over the past two years. Our findings show that after initial cloud technology adoption, there is a shift between public and private cloud consumption, driving the need for hybrid solutions. Our session will introduce Nutanix Calm for application-centric IT automation to drive both on-premise and off-premise workloads, delivering choice, self-service application governance, and automated life cycle operations.

Join us to learn how hybrid cloud capabilities combine benefits of on-premises infrastructure for predictable, mission-critical applications and public clouds for elastic, unpredictable workloads.

Wednesday

Cognitive Cyber Security
Mr. an Doyle
IBM
1000 – 1045 River Rm 1

The capabilities of Blockchain are starting to impact US Government and DoD business networks. How can you get a better sense of what Blockchain is, how it will be leveraged by government and what is the technology
Industry Seminar Details

behind it? Will you be participating in commercial blockchains, standing up a blockchain to solve a tactical problem, or bringing together a business network to consider transformation of a current business process leveraging blockchain to provide new value to all participants?

This session will explore the basics of Blockchain, explain why a permissioned blockchain is the right answer for government, and investigate key use cases in pilot/production where the promise of blockchain capability is being realized today. IBM will also provide an overview of how to start with blockchain technology in order to allow your organization to prepare to leverage the trust, transparency, and accountability that blockchain can bring to your business network.

Constantly Connected: Cybersecurity and a Digital Native Generation That Shares Everything

Mr. Paul Wamsted
IndraSoft, Inc.
1055 -1140 River Rm 1

If you’re online, you’re a soft target for our enemies. What does it mean to our youngest generations to grow up “online,” sharing extremely personal information as the norm? Air Force (USAF) members and their families face the same dangers online, but are additionally targeted for their access and critical force knowledge. How can the USAF create an environment of holistic cybersecurity where security training begins early in life? We communicate to our children the dangers of talking to strangers, but what about the day-to-day dangers of online interactions? The USAF is uniquely positioned to increase cyber awareness among its members and their families, creating an environment that stresses cybersecurity from a young age. As we move deeper into the 21st Century, the USAF will be reliant on these younger generations for personnel and support. How can we foster those discussions to prepare for cyberattacks now?
Monday

The Vision and Mission of the AFEA
Ms. Sloane Bailey
1040 – 1125
Alabama D

Can you spell “E-A”?! Well, whether you can or can’t, stop by this session to hear Ms. Sloane Bailey, Chief, Enterprise Architecture (EA) Division, SAF/CIO, outline the vision and mission of the USAF Enterprise Architecture, including initiatives underway, future components and capabilities, and the vision for the future of the AFEA.

ID Data Management
Mr. Scott Poole
1040 – 1125
Montg Rm 9

ID data management services can do for other programs, and how to get in contact with us/submit a request for our assistance.

Enterprise Configuration Management - Auditing
Capt Mark Lebedzinski
1040 – 1125
Montg Rm 5

The purpose of auditing is to “know thyself”, i.e., to ensure Enterprise systems are deployed and maintained in accordance with established baselines thereby ensuring IT Services support agreed performance levels for business and warfighting customers. The initial auditing capability focused on the AFNIC-managed core enterprise services portfolio for configuration, performance, and architecture health. Auditing is a sub-task of the Defense Enterprise Service Management Framework (DESMF) Configuration Management process.

Proper Configuration Management requires validation and remediation to maintain a healthy enterprise. AFNIC SME’s will provide a Demonstration and familiarization training for NOSC, MAJCOM/Base, and PMO technicians on how to use the established Baseline reports located on AFNIC’s System Center Operational Reporting Environment (SCORE): https://cs.eis.af.mil/sites/10026 to support their efforts to maintain the health of the AFNET. It’s a team sport!

Spectrum Policy for Unmanned Systems
Mr. Yash Sinha
1040 – 1125
Montg Rm 7

Unmanned aircraft represent a sector of aviation that will undergo exponential growth over the coming years. Unmanned Aerial Systems (UAS) are the new threat that the military have to find ways to defeat. The spectrum plays a big part in preventing the threat of UAS. This track will provide the status on new policies, and highlight the new R&D areas that are required to support the USAF in combating the UAS threat. We will also provide up-to-date information on the changing landscapes of UAS and ask the audience to participate by providing input into formulation and execution of these policies in today’s complex environment.

Enterprise Level Security
Mr. Frank Konieczny
1040 – 1125
Montg Rm 6

Enterprise Level Security (ELS) is a novel Identity and Access Management (IdAM) system that is being piloted by the USAF as the IdAM solution for the DoD Joint Information Environment. ELS lets applications grant and restrict access to users based on their authoritative attributes (e.g., job position). The system can then dynamically modify the user’s access to appropriate applications/data as Airmen change jobs, thereby providing an additional layer of security at the application/data level without increasing the workload placed on system administrators. This session will discuss ELS’ components and interactions, the generation of claims from attributes, the auto-provisioning of applications to the cloud, and provide insights into the planned capabilities regarding multi-factor authentication mechanisms and unstructured data access.

Blue Horizons: Technology, Strategy, and the Future
Col Jeffrey Donnithorne
1040 – 1125
MPAC

Blue Horizons is a CSAF-chartered IDE/SDE program at Air University, focused on the integration of strategy and technology for the future Air Force. This presentation synthesizes ideas recently discussed in the program, with
an emphasis on (1) identifying the broad trend lines shaping the future and (2) the types of investments the Air Force should make to prepare for a range of possible future. Two global trends receive primary focus: the great migration (the movement of human ecosystems into the digital world) and the great convergence (the increasingly blurred space between digital and physical reality). To prevail in the fast future, the Air Force needs to prioritize connections and networks of all types, develop expertise in algorithms and human-machine teams, and foster a culture that once again thinks like a challenger, not a reigning champion.

**Information Dominance Governance**
Mr. Ben Yarish
1040 – 1125  
**Alabama E**

Governance plays a critical role to ensure alignment between strategy, resources and operations. SAF/CIO-A6 is responsible for policy, strategy, and the oversight of Information Dominance to support AF core missions. Effective Governance is critical to ensure information technology/cyber support to key mission areas and Capital Planning and Investment Controls. The role of MAJCOM/A6s and HAF/SAF Functionals is key for successful Governance to deliver needed capabilities to Airmen.

**Continuum of Learning: Cyber Training in the 21st Century**
Col Robert Thompson
1040 – 1125  
**Montg Rm 4**

The USAF is pursuing a strategy to bring cyber training from the Industrial Age to the Information Age. This strategy seeks to modularize Initial Skills Training and present relevant, robust, flexible, and portable education opportunities. The model moves away from “instructor lead” presentations and towards Distance Learning, Blended Learning, and Upside-Down Classroom models. Furthermore, we’re pursuing cloud-hosted training repositories which move us toward the end-state of a Continuum of Learning across a member’s career.

**Common Computing Environment (CCE) & GCSS - Status Update and Way Ahead**
Col Steve Dinzart, Mr. Michael Plattele, Mr. Jim McGovern
1135 – 1220  
**Montg Rm 9**

**Cybersecurity Perspectives for Cyber-Physical/Control Systems**
Col David Stone
1135 – 1220  
**Alabama E**

Cyber attacks that cause physical damage or affect physical processes are no longer limited to theory or speculation. Traditional cybersecurity and defensive cyberspace operations remain challenged in their own space, and they are even more taxed in cyber-physical/control systems environments. Alternatively, top-down, purpose-based approaches to preventing unacceptable losses and consequences resulting from malicious cyber activity allow an organization to apply limited resources to critical, key elements of their operation without necessitating a need to cover the entire waterfront.

**IT Executive Panel**
Mr. Bill Marion, Maj Gen Sarah Zabel, Mr. Arthur Hatcher, Mr. Stuart Timerman, Mr. John Gilligan
1135 – 1220  
**MPAC**

The purpose of this panel is to hear executive leadership perspectives on how they are incorporating emerging information technology into their respective organizations.

**Air Force War Planning and Execution Agile Journey**
Mr. Glenn Bright, Ms. Tanisha Perry, Mr. Gene Evans, Mr. Tom Stubblefield, Ms. Vivian Martin
1135 – 1220  
**Montg Rm 7**

The Air Force’s premier system Program Management Office for War Planning and Execution (WPE) embarked on an Agile journey with its flagship software, Deliberate and Crisis Action Planning and Execution Segment (DCAPES), and its future WPE software deliveries. The purpose of this presentation is to share that experience and lessons learned from perspectives including test planning, development process, and project metrics.
Government Seminar Details

Automated Remediation and Asset Discovery (ARAD)
*Closed*
Ms. Denise Hampt, Ms. Robin Mason, Ms. Jessie Mues,
Lt Col Bradley Panton, Ms. Deb Moorehead
1135 – 1220 Montg Rm 8

Automated Remediation and Asset Discovery (ARAD) was established to meet requirement criteria for vulnerability management execution, defensive cyberspace operations, problem resolution, asset management, and situational awareness. ARAD executes capabilities supporting USAF enterprise endpoints. This presentation will demonstrate USAF use of this capability.

38 Engineering Squadron: Providing Engineering Services to Enable the Cyber Domain
Mr. Stephen Mitchell
1135 – 1220 Alabama D

The primary mission of the 38th Engineering Squadron is to establish, extend, and support cyberspace enterprise infrastructure by base-lining, planning, designing, establishing, expanding, optimizing, and/or replacing cyberspace systems. The 38 ES provides expertise to design, engineer, install, configure, and test the full range of cyber infrastructure systems, equipment, and components typically found at main operating bases as well as other specialty systems unique to expeditionary and strategic communications forces.

The 38 Engineering Squadron also provides the following specific Cyber engineering capabilities to the AFNET and AF bases:
1. Develops AFNET standards (such as the AF BAN Functional Specification);
2. Integrates AFNET standards into base network designs to support mission assurance;
3. Evaluates AFNET technical standards compliance for base networks (and provides recommended solutions for non-compliant items);
4. Implements/employs AFNET standards at AF bases (includes troubleshooting and optimizing AFNET Enterprise and base level network configurations).

A Home for EA: Where does architecture fit in the organization?
Maj Gen Patrick Higby
1135 – 1220 Montg Rm 5

Maximizing the impact of Enterprise Architecture (EA) in an organization is largely a function of where it sits. Yet too often, EA is pushed into the Information Technology (IT) department, where documenting IT eco-systems becomes the focus, rather than using EA to document critical paths to business and/or mission execution. EA does not just model systems; it models people, process, data, interactions, and technology. This discussion is aimed at dispelling common myths, and moving EA to a place where it has a more “holistic” view of organizational mission execution, of which IT is but one critical part.

Base of the Future
Maj Adrian De Freitas
1135 – 1220 Exhibit Hall

What will the base of the future look like? In this panel, we bring together subject-matter experts from across the USAF to talk about our plans for modernizing our aging bases for the 21st Century. We will discuss technologies such as 1) mobile connectivity (e.g., LTE), 2) alternative desktop platforms, and 3) Internet-of-Things devices, and how they will change the way that Airmen accomplish their missions. Additionally, we will host an open discussion to see what impact, if any, upcoming technologies such as artificial intelligence and virtual/augmented reality are expected to have. Audience members will have a chance to engage with the panel and propose their own ideas, so make sure to leave conventional thought at the door!

COTS Technology Based Solutions to “Wicked” Infrastructure Security Problems

Smarter Cities/Smarter Bases
Mr. Boyd Stephens
1250 – 1350 Brown Bag Montg Rm 9

Within the never-ending game of the criminals one-upping particular products, services and vendor solutions, customers of technology-based solutions often end up on the receiving end of an attack or vulnerability threat that
they are unable to directly address. Many issues are due to their being beholden to a respective vendor’s not disclosing its “secret sauce” or not being privy to the details of a particular “proprietary technology.”. The U.S. Air Force is not immune to any of these circumstances where in some capacity it may be among the most vulnerable of targets. Unlike other warfare domains, the domain of Cyber is unique in one particular manner — the enemy is not required to possess vast amounts of wealth nor access to vast resources that are inaccessible to most in order to wreak global havoc. Within the world of IT and Smarter City/Base deployments, these types of challenges increase by multiple orders of magnitude. Open systems, standards, and services, when combined with COTS (Common Off The Shelf), hardware technology can be heavily leveraged in mitigating many of these challenges.

The Future of Dial Tone
Mr. Victor Byrum, Ms. Rachelle Burns, Ms. Eleanor Zachery
1250 – 1350 River Rm 6

38 CONS is the Air Force’s central focal point for local commercial telecommunications contracting, and has recently held multiple industry days to discuss what industry would like to see in a Request For Quote (RFQ), how they can accept payment (i.e. Wide Area Work Flow), and how to evolve to performance-based requirements that will allow for innovative solutions to update the Air Force’s aging infrastructure at the best value in a competitive environment.

Discussion will include the CIPS process in building CSA requirements packages, a checklist of required documents (including a Performance Work Statement (PWS), Requirements Approval Document (RAD), certified funding in the form of an AF Form 9 or MIPR, and a green procurement form), sample templates and links to those templates, and changes in technology, policies and acquisition process.

Integrated Cyber Defense of USAF Weapons Systems
Col Bill Byant
1250 – 1350 Montg Rm 6

The USAF core missions are completely dependent upon systems that operate in cyberspace, but most of our systems were designed for a completely different world, not the cyber-contested environment we expect to face. USAF systems can be categorized as traditional IT, Operational Technology (OT), and platforms such as aircraft. Across all of these systems, the best defense includes a combination of traditional IT-based defense in depth, resiliency, and active defense. None of these approaches can be effective without the other two and they must be fully integrated.

There are a number of measures that can be taken in the short, mid, and long term to much more effectively defend our cyber-physical systems.

S&T for Air Force IT
Maj Adrian De Freitas
1250 – 1350 Alabama D

Since 1997, USAF research has played a key role in ensuring that we continue to deliver novel technologies and capabilities to the warfighter. This tradition is carried through today with projects supported in the USAF Science and Technology (S&T) portfolio. In this session, we will present an overview of the research efforts conducted in support of cyber concerns throughout the USAF, including Cyberspace Superiority. We will include selected short presentations of efforts that have been or are being transitioned in the USAF enterprise, and provide our short and long-term research goals.

Transitioning Systems to the Risk Management Framework
Mr. Kevin La Salle
1250 – 1350 River Rm 3

The USAF Chief Information Officer (SAF - CIO A6) will host this informational session on the AF transition to and implementation of the Risk Management Framework (RMF) as mandated by the Department of Defense (DoD). Transition to the RMF is a responsibility of the entire federal government and must be fully implemented for all AF Information Technology (IT) by April 1, 2018.

Clinger-Cohen Act
Lt Col Francis Tyson
1250 – 1350 River Rm 2

The Clinger-Cohen Act (CCA) certification process is part of the deliberate and iterative plan that will ensure the USAF
ability to efficiently and effectively acquire IT while integrating CIO Strategic Priorities early in the acquisition process. This session will focus on providing an overview of the implementation plan for reforming and streamlining the CCA certification process. Additionally, the team will discuss how CCA will be implemented for business systems in the new DoDI 5000.75, Business Systems Requirements and Acquisition, dated 2 Feb 17. Program Managers, Portfolio Managers, Functional Sponsors and CIO compliance staff/SMEs discussing CCA specified and implied tasks to ensure success while remaining compliant with statutory requirements are invited.

Spectrum Supporting Virtually Every USAF Operation
Col David Bosko
1250 – 1350  Alabama E

This forum will discuss that spectrum underpins every CSISR network and enables freedom of maneuver in the Cyber domain. The electromagnetic spectrum enables operators to conduct the full range of military operations around the globe. To safeguard our CSISR networks and protect our mission capabilities from external pressures and threats, we must assess, acquire, and protect our spectrum dominance. Attendees will better understand what role spectrum plays in global operations; how a lack of spectrum planning can thwart capabilities; what spectrum threats exist; how we must incorporate more spectrum engineering into our acquisitions and development processes to build more spectrally efficient and agile systems that will make systems like the Joint Aerial Layer Network (JALN) more powerful for the warfighter.

The Cyber Threat and Way Ahead
LTG (Ret) Ronald L. Burgess, Jr.
1250 – 1350  MPAC

A discussion on the cyber threat to the United States and our national security in an inter-connected world. The role of government, private and public companies and academia.

How to Integrate EA Further into AF processes
Ms. Carolyn (Hope) McMahon
1250 – 1350  River Rm 7

An open discussion between architects and consumers to determine the best ways to “de-mystify” Enterprise Architecture (EA) and determine what steps should be taken to get more visibility and support for EA activities at all echelons of the USAF and in support of more than just technology solutions.

The Future of EA
Ms. Sloane Bailey
1250 – 1350  River Rm 4

Enterprise Architecture (EA) is being used by Fortune 500 companies, as well as government agencies with substantial budgets to identify areas for efficiency, investment, and transformation. As these organizations move to a data-driven model for representing and analyzing EA, they are also looking to the next evolution of how to represent and use EA to provide that next “edge” in their marketplace or area of responsibility. This will be an interactive discussion about how leading users of EA are applying the current trend of data-driven architecture to improve forecasting and decision-making at all levels of their organization. Additionally, we want to hear what trends are on the horizon that they feel set the stage for the next big leap, such as behavioral and insight/intent-driven.

Operationalizing Enterprise Architecture (EA)
Ms. Teresa Ooth
1250-1350  River Rm 5

The operationalization of Enterprise Architecture is vital to understanding your Enterprise and setting a course for how your mission will be accomplished in the future. This breakout session is an actual case study of how the AMC Enterprise Architecture Office used DoDAF compliant architecture artifacts to answer the HQ AMC/A3 Deputy’s operational requirement to restructure the roles and responsibilities of the planners in the 618th Air Operations Center (AOC).

Leading Innovation at AF CyberWorx
Col Jeffrey Collins
1250 – 1350  Montg Rm 7

In 2016, the Air Force stood up CyberWorx, a venture comprising a public-private research and design center focused on cyber capabilities and disruptive technologies.
A small, innovative team melds military, academic, and industry expertise with state of the art technology and user-centered design to solve tough operational problems for the DoD. CyberWorx also enhances cyber education for officers in a creative problem-solving environment with an inclusive student demographic. This presentation will describe the problem-based learning approach; how CyberWorx partners with industry to deliver innovative operational cyber solutions to Air Force and Joint commands; and the cultural changes CyberWorx is leading to help the Air Force become more agile and innovative. This talk will also serve as a primer for those wanting to understand “design thinking” as one of the problem-solving approaches digital-native cadets learn at the USAF Academy.

Blue Horizons is a CSAF-chartered IDE/SDE program at Air University, focused on the integration of strategy and technology for the future Air Force. This presentation synthesizes ideas recently discussed in the program, with an emphasis on (1) identifying the broad trend lines shaping the future and (2) the types of investments the Air Force should make to prepare for a range of possible futures. Two global trends receive primary focus: the great migration (the movement of human ecosystems into the digital world) and the great convergence (the increasingly blurred space between digital and physical reality). The presentation then highlights three broad categories of investment to prepare for the future: connection, code, and culture. To prevail in the fast future, the Air Force needs to prioritize connections and networks of all types, develop expertise in algorithms and human-machine teams, and foster a culture that once again thinks like a challenger, not a reigning champion.

**A Proof-Of-Concept Demonstration of Application Layer Cyber Security System Dynamics Modeling**

Dr. Uma Kannan

1250 – 1350

River Rm 1

System dynamics (SD) is a methodology used to understand how the components of a system interact and how the systems change over time. SD is developed to solve long-term, chronic, and dynamic industrial management problems. SD is predominantly used to solve various business policies and strategic problems. This paper presents a study which models a computer network as a systems dynamic model to explore cyber-attacks and the resulting system-level effects that might occur on the host OSI layers, layer 4 and above, from the OSI model. Computer networks are normally modeled or simulated through discrete-event techniques. But the primary focus of discrete-event simulation is on packet traffic. This means that cyberattacks/defenses are viewed from the network layer, layer 3, in the OSI model. Preliminary results indicate that by using system dynamic cyber security simulation, an organization can imitate the attacker activities in the OSI layer 4 and above and assess (and/or mitigate) the system’s exposure to risks. We describe the cybersecurity model’s simulation results and compare it with a cyber attack on a real system.

**IT Acquisition**

Maj Gen Sarah Zabel, Ms. Lauren Knausenberger, Mr. Jason Hanson

1250 – 1350

River Rm 8

With Software as a Service (SaaS), cloud capabilities, and the need to unleash the power of innovation, our standard methods of IT acquisition must be revised. At the same time, increasing cyber challenges and the imperative to operate and support the systems we field re-emphasize the necessity of methodical testing and effective security. The USAF has embarked on pathfinder efforts to bridge from traditional acquisition to a new, more responsive approach, but there are still many gaps in our processes. IT Acquisition is an interactive panel focusing on new approaches to acquisition to bring capabilities to bear for the warfighter. While agile development processes are well-established in industry and pockets of DoD, the bigger challenge of taking new capabilities from idea through testing, accreditation, deployment, operations and support, still lag the need. This panel will address the status of current pathfinder efforts and look for new approaches to capability development and deployment.

**Tuesday**

**AF Data Management**

Maj Gen Kimberly Crider

1030 – 1115

MPAC
Today’s most successful organizations are literally data-driven. From the most senior levels on down, in and across every function, these organizations use data in highly intentional, systematic ways to seize opportunities, resolve strategic challenges and create competitive advantage. What sets these organizations apart is that they view data as a core asset, and they have established a scalable framework and adaptive culture that enables data that is visual, accessible, understandable, linked and trusted for meaningful analytics and decision-making. In this interactive breakout session, we will talk about the approach the AF is taking to becoming a data-driven organization, and the role you can play, not only in its rapid evolution, but also in using data and analytics to create value in all AF mission areas.

**Joint Regional Security Stack (JRSS)**
Maj Philip Wachlin
1030 – 1115
Exhibit Hall

The Joint Regional Security Stacks (JRSS) is our first major step in achieving the long-sought vision of the Joint Information Environment (JIE). This new joint platform is being deployed on both NIPRNet and SIPRNet and is the future of how the USAF will conduct boundary protection at both the local and regional levels in a cyber contested environment. During this session, representatives from the operational units up to Headquarters Air Force will hold a panel discussion. We will cover items such as the current status of migrations, where this initiative will take us in the future, funding, and how this helps the USAF to get closer to JIE. The topics are not limited to these items and will be driven by the questions and interactions we get from the field. Please take the time to stop by, learn, and ask questions!

**Agency Catalog and Reporting**
Ms. Joanne Woytek
1030 – 1115
Alabama A

Curious about how NASA SEWP's Innovative Agency Catalogs and Reporting capabilities simplify the procurement tasks of all Federal Agencies? Then attend SEWP’s interactive audio/visual presentation! Agency Catalog topics covered: what they are, when to use them, how they are implemented, and how to get one created!

Also being presented is our innovative approach to meeting federal agency reporting needs. Find out how your federal agency can receive bi-monthly reports on where and what was purchased, pricing, category, reseller, and manufacturer. Data collected for Agency Reports: Contract Line Item Number (CLIN) data and Federal requirements of EPEAT, TAA, Supply Chain Risk Management, etc. Currently, there are 27 points of data collected and available for reporting. Agency Catalogs and Agency Reporting provides federal agencies with fast, simple IT procurement, tracking, and reporting. No other federal contract vehicle provides these capabilities to federal organizations.

**DoD IT Strategic Sourcing – DoD Enterprise Software Initiative, OMB Category Management, and Strategic Vendor Management**
Mr. Floyd Groce
1030 – 1115
Montg Rm 5

Session will provide an overview of DoD IT strategic sourcing landscape, including DoD Enterprise Software Initiative (ESI) efforts and federal-wide expansion through OMB’s Category Management (CM) Initiative. We will review lessons learned for successful Strategic Vendor Management (SVM) and negotiation of End User License Agreements (EULA) to highlight key government considerations for commercial IT procurements.

**Mission Threads and Service Core Functions**
Mr. Steve Glazewski, Ms. Carolyn (Hope) McMahon
1030 – 1115
Alabama B

Regardless of whether the focus is on the “big” picture or on a single solution, Enterprise Architecture (EA) supports decisions at all levels. If completeness of models or artifacts does not imply validity, then how can decision-makers be sure that they are receiving value from the architecture? We will discuss both the vertical organizing construct using the Air Force’s Service Core Functions (SCFs) and, perhaps more importantly, the horizontal organizing construct of “Mission Threads.” These threads combine to represent what is valued and relevant across the USAF. Integrating these threads into the EA positions the USAF to support critical decisions by senior leaders.
Government Seminar Details

**Records Management of the Future**  
Lt Col Francis Tyson  
**1030 – 1115**  
Montg Rm 6  
This session will focus on providing an overview of the new Interim Change (IC) to AFI 33-322, Records Management Program, dated 25 May 2017. It will be geared towards communications squadron commanders discussing Records Management specified and implied tasks to ensure success while remaining compliant with statutory requirements.

**The Air Force Spectrum Strategy 2030**  
Mr. Yash Sinha  
**1030 – 1115**  
Montg Rm 7  
In today’s competitive global market, smart strategies are more critical than ever before. Assured spectrum access is vital to maintaining our national security, military superiority, and responsiveness to events that challenge our interests at home and abroad. Spectrum military leaders need to build interagency and industry complex partnerships to meet the nations’ objectives in this congested spectrum environment. The USAF is at an increasing disadvantage in securing spectrum bands as it is combating pressures from Congress, industry and adversaries. The audience will be able to provide input into formulation and execution of the USAF strategy in today’s complex, competitive and congested global spectrum environment.

**Education with Industry**  
CMSgt Denzil Hellesen, Mr. Mark Hanson  
**1125 – 1210**  
Montg Rm 4  
Education with Industry, more commonly known as EWI, is as old as the Air Force. It is a primarily an acquisition’s education program run by the AQ Directorate on the Air Staff. Since 1947, EWI was by design, and execution an officer and civilian development program, focused on bringing seasoned CGOs and civilians out of their primary functional areas, PCSing them to industry to learn how those industry partners “handle” acquisitions from a corporate view. Until now...Since 2015 4 enlisted cyber Airmen have gone to work with companies like VMWare, Microsoft, and USAA to learn how they provide, secure, and defend their cyberspace from the “enemy,” and have brought that experience back to our ranks. Come hear the story.

**Civilian and Cyberspace Career Development**  
Mr. Bill Marion  
**1125 – 1210**  
MPAC  
Here’s a great opportunity to participate in an interactive session with the most senior civilian in the Air Force's nearly 15,000-member Communications and Information career field. You’ll hear remarks on the 24AF transition and Enterprise IT, as well as leadership perspectives on the 2017 Information Dominance Flight Plan and the value of mentoring. Other topics include the latest status on Civilian Fast-Track Cyber Hiring, implementation of the Cyber Exempted Service, and the upcoming Department of Defense Chief Information Office led initiative to code the cyber workforce using the Defense Cyber Workforce Framework. Nearly half of the session is dedicated to interaction with the audience...so bring your questions!

**Development Opportunities in the CCE**  
Col Steve Dinzart, Mr. Michael Platteel, Mr. Jim McGovern  
**1125 – 1210**  
Montg Rm 5  
**CIPS Update**  
Mr. David McKeever  
**1125 – 1210**  
River Rm 8  
The Cyberspace Infrastructure Planning System (CIPS) Program Office will update AFITC attendees on the latest efforts to modernize CIPS (ver 5.0). A brief background will be given, followed by a showcase of the most recently deployed tools: Work Order (WO) and Work Flow (WF). CIPS WO replaces legacy Work Order Management System (WOMS). It provides workload management for Base Work Center assigned tasks, supports O&M activities of existing infrastructure, and is highly flexible and customizable. This overview will describe structure, function, and the underlying security.

CIPS WF replaces the legacy CIPS Routing Slip. This presentation will describe the new WF informational routing capability, illustrating its features as a Staff Summary sheet that allows routing to select users within CIPS. It can stand alone or can be used to route attached...
documentation. Please visit the CIPS booth (#565) on the
showroom floor for additional information
and/or demonstration.

**AF Information Technology Commodity Council (ITCC)/Network Centric Solutions-2(NETCENTS-2)/AFWAY: Strategic Sourcing for the 21st Century**
Mr. Laurence McGraw, Ms. Gena Howard, Mr. Dennis Notareschi
1125 – 1210 Montg Rm 9

Are you planning on purchasing IT products and/or services and don't know where to begin? The AF ITCC, NETCENTS-2, & AFWAY are the enterprise solutions for strategically sourced IT commodities and services that support AF and DoD initiatives like IT Category Management and BBP 3.0. Information will be presented that will help you understand these enterprise solutions and how to utilize them to meet your organization’s needs while ensuring compliance with applicable mandatory use procedures.

**Enterprise Information Technology as a Service (EITaaS)**
Col Douglas Dudley, Col Charles (Paul) Young
1125 – 1210 Exhibit Hall

The Air Force has five core missions: 1) Air and Space Superiority, 2) Intelligence, Surveillance, and Reconnaissance (ISR), 3) Rapid Global Mobility, 4) Global Strike, and 5) Command and Control, all of which require access to effective Enterprise Information Technology Services. Ensuring AFNET capacity and capabilities are sufficient to meet the needs of the Air Force’s growing and evolving mission is a significant challenge. By leveraging industry to meet this challenge, the Air Force warfighter will benefit from commercially proven technology resulting in more efficient and effective services at a reduced price. Learn about how the Air Force plans to leverage industry to provide Enterprise Information Technology services.

**Interoperability through Enterprise Architecture**
Lt Col Jeremy St. Louis
1125 – 1210 Montg Rm 6

Stove-piped systems mean you stand alone in today's interconnected digital world. Efforts are underway to realign requirements criteria and processes to integrate interoperability throughout capability development. This session is a discussion on how these actions are moving forward, and an opportunity for the USAF community to weigh-in on the changes that will directly impact their programs.

**“Cyber Snake Oil Sale—today only” AKA, The most common fallacies of the cyber-security marketplace**
Col Clint Mixon
1125 – 1210 Alabama B

The talk will discuss the serious logic flaws in the most common cyber-security thought processes and products. Specific fallacies covered will include: Cyber Risk Calculations, Cyber Key Terrain, Five 9’s, Redundancy, Inventory/Physical layer approaches, Anti-Virus Programs,

**Mobility**
Maj Adrian De Freitas
1125 – 1210 Alabama A

This session will provide an overview of the 5 lines of effort currently underway under the auspices of the USAF Mobility Enterprise Services PanelBase Wireless Capability that focuses on providing connectivity for voice, data, video to NIPRNet and SIPRNet for mission and business applications; Platform Wireless Capability focusing on platform wireless services and capabilities; Device Lifecycle Management for endpoint, client-side, device lifecycle management including selection, issuance, provisioning, sustainment, and disposition; and, Mobile Mission Integration supporting both protocols and device assimilation across wireless joint, commercial and private network/information domains. The session will give audience members a chance to comment on current projects, as well as recommend areas for future consideration.

**Tactical Cyber Survivability**
Col Jeremy Boenitsch
1125 – 1210 Montg Rm 7

Tactical cyber survivability is paramount to C5 ISR communications and warfighter effectiveness in contested environments. We must continually assess how we will
Government Seminar Details

communicate when tactical communications are unavailable and we must educate our mission partners on Primary, Alternate, Contingency, Emergency (PACE) planning. This session will discuss the importance of tactical cyber survivability and processes and procedures that can be adopted to enhance the mindset and culture in this area.

Small Business Forum
Ms. Denise Baylor
1230 – 1600 Alabama A
Half-day sessions covering small business topics.

Organizational Roles / Responsibilities for EIT Services
Col Charles (Paul) Young, Col(s) Gerald Yap
1545 – 1630 River Rm 4
Learn how clarifying roles and responsibilities of EIT Service Delivery Teams in providing services to the USAF in providing EIT Services changes everything. Topics to include:
- Substantive changes to organizational roles and responsibilities normalize enterprise IT governance with AF corporate structures
- Organizational roles/responsibilities in EIT create a Team of Teams focus to providing Enterprise IT to the Missions
- Providing dedicated resources to interface with and understand the Mission Requirements
- Roadmap for process design and implementation opportunities for process automation aligns IT Service delivery with industry best practices and DOD guidance

Windows 10
Mr. Lamar Hilton
1240 – 1340 Alabama B
Overview of the Standard Desktop Configuration (SDC). Windows 10 has been mandated by the DoD CIO for all services to defend against modern security threats. The operating system introduces a completely new servicing model resulting in new features and updates being provided much sooner than previous operating systems versions. Continuous application compatibility efforts against mission systems will be required to ensure mission readiness and consistent operational availability. Modern features of the SDC focus to mitigate current cyber threats to endpoint devices before being incorporated into the SDC for enterprise implementation.

The Language of the Enterprise Lexicon and Taxonomy
Lt Col Jeremy St. Louis
1545 – 1630 Montg Rm 5
Attributes, data tags, and mission elements...what do they all mean? More to the point, how do you ensure they mean the same thing to people from different backgrounds and skill levels? Establishing an enterprise lexicon ensures continuity and standardization of elements across all levels of architecture. This session will focus on the need and best practices for implementing a common dictionary and enterprise lexicon for architectures.

CTO Forum
*Closed*
Maj Adrian De Freitas
1545 – 1630 Montg Rm 4
This is a by-invitation only session for Chief Technology Officers (CTO) from the MAJCOMs and functional organizations to speak with the USAF CTO. If you would like to attend this session, please contact the CTO office at usaf.pentagon.saf-cio-a6.mbx.saf-cio-a6-workflow@mail.mil.

Identity Assurance and PKI Panel
Mr. Rick Moon, Ms. Kit Nowell, Ms. Denna Price, Mr. Joe Tramont
1545 – 1630 River Rm 1
This is a by-invitation only session for Chief Technology Officers (CTO) from the MAJCOMs and functional organizations to speak with the USAF CTO. If you would like to attend this session, please contact the CTO office at usaf.pentagon.saf-cio-a6.mbx.saf-cio-a6-workflow@mail.mil.

Women in Government Service - Career Development
Ms. Essye Miller
1240 – 1340 MPAC
Ms. Essye Miller, Deputy CIO for Cybersecurity, Department of Defense will host a mentoring session with women in government service to include enlisted, officers and civil servants. She will discuss opportunities, challenges, and valuable advice for those navigating through their career paths. This is an excellent opportunity to learn from an Information Technology leader who has served in the USAF, Army and at the DoD level.
Government Seminar Details

This panel is comprised of experts from the Identity Assurance Section at The Cryptologic and Cyber Systems Division (CCSD) and the Air Force Public Key infrastructure (PKI) Program Office to discuss current and future efforts regarding strong identity assurance capabilities. Featured discussions showcase specific examples that leverage PKI to ensure integrity and security of sensitive information beyond traditional use-cases, such as email and smartcard logon, and present expertise regarding derived credentials for mobile technologies, public key enabling of legacy systems, and certificate delivery methodologies.

Working Together: Enterprise Architecture and Acquisition
Maj Gen Sarah Zabel, Ms. Carolyn (Hope) McMahon
1545 – 1630
River Rm 2

Every good builder counts the cost before embarking on a project to know and understand what is currently available and what will ultimately be needed. Prior to a procurement, it is important to understand the redundancies, gaps, and inefficiencies that may currently exist, in order to ensure that the right capabilities are integrated, thus bringing value and relevance to the mission. An operationalized architecture that leverages a repository and analysis tools further strengthens and enables the evaluation and appraisal of an organization’s competencies. This, in turn, facilitates the portfolio review process, as well as, empowers the management and control of the acquisition life-cycle, hence, the significant relationship of enterprise architecture and acquisition management working together towards common goals and objectives. Enterprise architecture, strategically integrated into the right stages of the life-cycle, assist with understanding these issues.

Panel Discussion on AFR Strategic Overview of Cyber Forces
*Closed*
Col Jerald Narum, Col Roberta Ernest, CMSgt Terrence Stokes
1545 – 1630
River Rm 6

The panel will provide an overview of Air Force Reserve strategic cyber initiatives, focus areas, talent management, information on the status of AFR Officer and Enlisted career field and an update on the AFR Cyber Squadron Initiative.

Negotiations in Today’s Environment
Mr. Stefan Eisen
1545 – 1630
River Rm 3

Today’s environment requires leaders to get things done working with people they have no direct authority over. Negotiations is a key skill for success in this environment. What makes for good negotiations? What gets in our way? What happens when you deal with a diverse team? Come to the seminar and get some insight on these and other negotiating issues.

The Threats of the Responsibly Imaginable
Dr. John Geis
1545 – 1630
River Rm 5

Within the field of Foresight Analysis is the concept of “Inevitable Surprises,” first coined by Peter Schwartz. These are events which are knowable or extremely likely, but because of their infrequency, it is our nature to not be prepared for them, and to act with surprise when they occur. This presentation will look at some of these impending “inevitable surprises” to include the challenges and opportunities of emerging drone technology as it pertains to communications, sensing and computing. It will look at the quantum revolution and what this may mean for military command, control, communications and computing. It will also look at infrastructure challenges to the homeland which may be tested by both terrorist and natural events over the next 20-30 years, and will discuss why the natural events may both be the more worrisome and the more likely challenges.

Ethics of increased technology and killing
Lt Col Robert Vicars
1545 – 1630
River Rm 8

Technology has long been used to enhance combatant capabilities on the battlefield. More recent technology, however, is being used to replace combatants on the battlefield. This change has produced some moral implications that are not completely obvious. In researching the ethics of killing in war, one encounters two distinct forms of moral reasoning—that based on common individual morality, and that based on collectives. This
Government Seminar Details

The seminar will summarize each and propose a different approach that is combatant-centric. This proposal outlines the groundwork for a theory of the combatant.

**AF Software Enterprise Acquisition Management & Lifecycle Support (SEAMLS): Evolving - Empowering - Enabling**
Mr. Ben Burns
1545 – 1630 River Rm 7

SEAMLS provides acquisition and license management of the Air Force Oracle & Gartner Enterprise License Agreements (ELAs); Adobe, Cisco, and Microsoft Joint Enterprise Level Agreements (JELAs); and the DoD Enterprise Software Initiative (ESI) Telos Blanket Purchase Agreement. Serves as the central focal point for AF Enterprise IT software requirements aimed to save money, streamline the acquisition process, facilitate enterprise licensing and improve information sharing.

**Modernizing Information Support Capability**
Lt Col Eric Trias
1545 – 1630 Alabama B

This breakout session features discussion on current AF initiatives to modernize information support capabilities such as e-Records, e-Publishing, Training and e-Learning.

**DISA Mission Brief**
Lt Col Brad Barnhart
1545 – 1630 Montg Rm 7

A “101” presentation of DISA senior leadership and the DISA services for which they are responsible.

**Preparing to Become a Smart City, Base of the Future Panel**
Panel (AMC, AU, Montgomery/AL, AT&T)
1545 – 1630 Exhibit Hall

In this session, panelists will be represented from all facets of the SmartCity/Smart Base equation. From the USAF’s infrastructure to its ability to educate its future cyber warriors, we would like to guide the discussion on the challenges and obstacles ahead in becoming a more efficient and innovative cyber force. Other panelists include representatives from organizations currently employing Smart City initiatives to the industry technologies leading them through the transition. Our hopes are to address lessons learned and way ahead. Our goal is for attendees to learn about how their installations and communities can prepare to become a Smart Base in today’s ever-changing and cyber-enhanced environment.

**USCYBERCOM Senior Enlisted Member**
CSM David Redmon
1545 – 1630 MPAC

**Wednesday**

**AF Enterprise IT Service Strategy**
Col Charles (Paul) Young, Col(s) Gerald Yap
1055 – 1140 Montg Rm 5

Don’t miss your chance to hear about the USAF CIO’s vision for Enterprise IT Service Management. The AF is overhauling its approach to deliver Enterprise IT Services and ensure they are mission relevant, cybersecure, and affordable. Take the opportunity to learn how these changes will improve mission effectiveness and give you direct input to shape future priorities. Topics to include:
- Role of mission and functional system owners in shaping EIT Service requirements
- New processes specifically to derive customer objectives and measure against those performance requirements.
- EIT Service Management integration with the Information Dominance Flight Plan goals and objectives.
- Alignment of AF EIT Service Management processes with the Defense Enterprise Service Management Framework (DESMF).

**Agile Airman Model (AAM)**
CMSgt Denzil Hellesen, CMSgt Lee Thul
1000 – 1045 Montg Rm 5

The USAF is implementing a new force management and force presentation model for our enlisted cyber Air Force Specialty Codes (AFSC). This model shifts required training from being “front loaded” in a member’s career to being presented on shorter portions at the right time. This model leverages modularized training and a Continuum of Learning environment to create Airmen with agile skillsets, versed in most recent, relevant technical and operational skills. Agile Airman Model (AAM) will support the
streamlining of cyber AFSC, eliminate redundancies in the delivery of cyber training, and provide career-long technical training/education for the cyber workforce.

Cyber Squadron Initiative (CS-I)
Lt Col Ryan Hampton, Mr. Joshua Neate
1000 – 1045 Exhibit Hall

Today’s Communications Squadrons will be fundamentally transformed into the Cyber Squadrons of tomorrow. These transformed squadrons will strengthen active, persistent cyber defense and mission assurance capabilities in support of USAF Core Missions. This initiative involves three interrelated lines-of-effort. First, it will build Mission Defense Teams to address persistent requirements. Second, the USAF must commoditize IT services (where possible) to allow existing personnel to refocus toward mission assurance. Finally, the USAF will change its culture and realign roles and authorities within the USAF portion of cyberspace. Our 45 Pathfinder squadrons are actively exploring the details necessary to accomplish this change.

Thinking Differently about Cybersecurity and Cyber Defense
Mr. Peter Kim
1000 – 1045 River Rm 4

The cyber threat has never been more serious than it is today, affecting every aspect of our professional and personal lives. Approaching cybersecurity and cyber defense differently, leveraging new ways of thinking about the problem and new technologies is fundamental to survival in today’s cyber world. USAF cyber operators blocked more than 1.3 billion malicious connections in 2016 alone, an average of more than 40 malicious connections per second. Nation state and non-nation state cyber adversaries are evolving faster than ever. We must think differently to get ahead of the threat for USAF mission assurance.

Officer All-Call
Maj Gen Patrick Higby
1000 – 1045 MPAC

Find out what’s happening in the Cyberspace Operations career field. Hear candid advice directly from the Career Field Functional Manager on the latest updates, changes and thoughts on a wide range of topics. Bring your questions too.

EA: Outside the Box
Ms. Aspasia Wooldridge
1000 – 1045 River Rm 5

The true power of Enterprise Architecture (EA) lies in the extent to which it can be leveraged in the common work environment. From impacting operational direction and processes, through identifying system linkages and impacts, to ultimately influencing decision making, EA provides many opportunities to lead the way in realizing organization potential. However, organizations are often challenged with how to employ EA to capitalize on its potential. This session will highlight examples where ‘out of the box’ forms of EA can be leveraged to support transformation efforts, portfolio rationalization and other CIO needs while looking at the related challenges, pitfalls, work-arounds and lessons learned and exploring with the audience ways to drive standardized and sustainable EA practices to drive organizational value.

ROI: EA-as-a-Service Model
Dr. Eddie Grimes
1000 – 1045 River Rm 6

Many times, architects are brought in by a program to build the program architecture and when it’s it is done, the architects are let go. The problems that this brings are there is no continuity of architecture skill, architecture is seen as one-and-done, and the focus is program-specific. When an organization provides "EA-as-a-Service", an office of architects is always available for architecture support which has many benefits. We'll highlight the many benefits of Enterprise Architecture-as-a-Service to an organization including corporate knowledge, enterprise perspective, consistency, time-savings and financial sense, and analysis that all lead to better-informed decision-making.

Continuous Integration & Software Quality
Mr. Scott Raley
1000 – 1045 River Rm 3

Continuous Integration (CI) is a software engineering practice in which isolated changes are immediately tested and reported on when they are added to a larger code base. The goal of CI is to provide rapid feedback so that if a defect is introduced into the code base, it can be identified and corrected as soon as possible. Teams leveraging continuous integration validate full lifecycle capabilities as frequently as possible. They develop, test, integrate, and
deploy every time they build. The more frequently teams perform all software lifecycle activities, the less likely it is that unforeseen high risk issues will surface unexpectedly. The PEO C3I&N Integration Branch Continuous Integration capability is a set of CI tools and processes designed to enable AF software applications to increase the overall quality and reduce the risk of developed software. This CI capability utilizes primarily open source tools including Jenkins, Maven, and SonarQube in order to make the benefits of CI available to AF programs at little to no cost.

**Educating for a Smart City, Base of the Future**
Panel (AU, USAF, AUM, State of Alabama, Microsoft)
1000 – 1045 River Rm 8

In this session, panelists will be represented from all facets of the Smart City/Smart Base equation. From the USAF’s educational senior leadership to local information technology education providers. We would like to guide the discussion on the challenges and obstacles ahead in educating our service members and community to become a more efficient and innovative cyber force. Other panelists include representatives from organizations currently employing Smart City initiatives to the industry technologists leading them through the transition. Our hopes are to address lessons learned and way ahead to best prepare our educational community for this transition. Our goal is for attendees to learn about how their installations and communities can prepare to become a Smart Base in today’s everchanging and cyber enhanced environment.

**Blockchain**
Capt Bradford Law
1000 – 1045 River Rm 2

Blockchain technology fully broke into the public eye with the success (and infamy) of Bitcoin. Cryptocurrency, and blockchain in general, represent just a small portion of the field of emergent distributed ledger technology. I will present the basics of blockchain technology, what makes it secure, the differences between privileged and unprivileged distributed ledgers, and the differences between public and private distributed ledgers. I also discuss possible future applications of the technology for private corporations, government, as well as consumers. Finally, I discuss my work on implementation of “Privilege”, my public key management proof of concept project implemented as a private, privileged distributed ledger.

**Two-factor Authentication (2FA)**
Ms. Deanna Price
1055 – 1140 River Rm 3

In accordance with USCYBERCOM TASKORD 15-0102, Implementation and Reporting of DoD Public Key Infrastructure (PKI) System Administrator and Privileged User Authentication, the AF PKI SPO has been tasked to review exemption requests for administrators/privileged users identified within every AF MAJCOM and provide a technical solution. Two-factor authentication requires privileged account holders to eliminate reliance on User Names and Passwords, ensuring a much stronger cybersecurity posture for our AF networks.

**Panel Discussion on AFR IT as a Service *Closed***
Mr. Michael J. Hess, Col Shane Matherne, Mr. Fred Massey, Mr. Clayton Sammons
1055 – 1140 River Rm 6

This panel will provide an overview of Air Force Reserve strategic vision, including mobile service delivery (personal and mission-related), Virtual Desktop and WIN10 compliance.

**Technology Innovation**
Maj Adrian De Freitas
1055 – 1140 River Rm 7

The USAF has a long tradition of embracing innovative technologies in order to deliver combat effects in air, space, and cyberspace. In order to stay on the cutting edge, however, the USAF needs a systematic process to match desired warfighting capabilities with novel technical solutions. In this session, we will present the USAF Chief Technology Office’s methodology for mapping use cases from the field into technical requirements for implementation, acquisition, and fielding. Our presentation will introduce the Consolidated Enterprise IT (CEIT) baseline, and discuss our strategy for categorizing technology vendor capabilities against known and/or projected mission requirements. We will discuss how we can leverage the latest technologies to meet the current and future needs of the USAF.
Government Seminar Details

**Evolving Spectrum Training**
CMSgt Lee Thul

1055 – 1140  Montg Rm 6

Globalization has made the world dependent on each other and it is the same for the USAF. As well, the spectrum utility and dependence will continue to grow for the foreseeable future. Furthermore, the spectrum manager role is also evolving as new threats and tools are identified. This session will focus on the evolving spectrum career field (3D1X4), by putting an emphasis on defensive operations and joint training with intel/cyber (IN2X1A).

**Enterprise IT Services in the Cloud: Hands off or hold on tight?**
Col Charles (Paul) Young, Col(s) Gerald Yap

1000 – 1045  Montg Rm 7

This is a workshop will use the USAF journey to cloud hosted messaging as a use case for exploring the role of IT Service Management. Topics to include

- In the move toward commercialization and multi-sourcing
- How are resource responsibilities determined?
- How are baseline and optional service levels/objectives determined?
- What does service operations mean in a broader commercialized environment?
- How hands-off can the AF become?
- What are the structural changes that make this happen?
- How are our joint responsibilities for situational awareness met?
- Does this make Enterprise IT Service Management obsolete?

**Application of EA to Cyber Security, Infrastructure, and Configuration Management**
Mr. Steven Stoner

1055 – 1140  River Rm 8

Enterprise Architecture (EA) is often viewed as just a “check box” along the way to funding or just merely a step in the requirements gathering process. There are three practical applications of “operationalizing” EA and using it to inform/support decision-making. We will hear from practitioners whom have leveraged EA to bolster their cybersecurity posture, to fortify their infrastructure investments, and to inform their change/configuration management practices.

**“Psyber” Conflict: Content, Cognition, and Connectivity**
Dr. Panayotis Yannakogeorgos

1055 – 1140  Montg Rm 7

The Internet is a critical tool that when unrestricted allows information to flow freely across the globe, opening the door to economic development, knowledge exchanges, and innovation. Broadband mobile technologies and digital informational and communication technologies augment decisions in the physical world. However, free flowing information can be used for enhancement of economic prosperity, aid in disaster response, enhance agricultural production based on data feeds, and better tracking of humanitarian assistance. These are all the result of emergent forms of networked societal behavior. However, these same technologies can target the human mind to influence a target population to either mobilize towards a collective goal, or intimidate and terrorize. This discussion focuses on “psyber” conflict - an illustrative term used to emphasize the convergence of content, cognition and connectivity.

**Why States Choose Cyber Attacks**
Dr. Andrew Akin

1055 – 1140  River Rm 5

Formal models of interstate conflict are a mainstay of the scholarship examining why wars happen. Vigorous empirical testing yields multiple theories on the origins of violent conflict between state actors. Cyber war however, challenges many of the bedrock assumptions of this research. Cyber war overcomes time and space constraints on kinetic operations and creates variable effects when implemented. This presentation addresses the tension between theories of conflict initiation for interstate and cyber war, and offers a new model for estimating why cyber war occurs.
**The AF IT Business Analytics Office**  
Mr. William "Butch" Luckie  
1055 – 1140 River Rm 4  

The AF IT Business Analytics Office (AF IT BAO) has been up and running since being established by the Secretary of the Air Force in January 2015. This breakout session will provide an update on the findings and progress made on “Bending the IT Cost Curve.” It will provide insight into the how the AF is implementing category management, from data collection through analysis, to help senior leadership make evidence based decisions on the procurement of information technology.

**Mission Assurance Decision Support System (MADSS)**  
*Closed*  
Mr. Joshua Neate, Mr. Bryan Reddan  
1055 – 1140 River Rm 2  

The Mission Assurance Decision Support System (MADSS) is a classified, centralized web-based tool that provides Combatant Commands, Services, and Agencies (CC/S/A) with an understanding of their mission dependencies on cyber infrastructure and near real-time and accurate situational awareness of the DOD Information Network (DODIN). MADSS addresses questions related to incidents affecting the DODIN (e.g., what capabilities are at risk, what capabilities remain, what are the alternatives, and how does this change the way we execute missions?). This brief will provide an understanding of the capabilities available in MADSS and how it is being used by the Air Force.