Advanced Distributed Learning Task 5(b) Cybersecurity Barriers to Distributed Learning Modernization Report

Potomac Institute for Policy Studies
901 N. Stuart Street
Arlington, VA 22203

The Potomac Institute for Policy Studies is an independent, 501(c)(3), not-for-profit public policy research institute. The Institute identifies and aggressively shepherd's discussion on key science and technology issues facing our society. From these discussions and forums, we develop meaningful science and technology policy options and ensure their implementation at the intersection of business and government.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
30-10-2018	Final Report	06-12-2018 to 30-10-2018

4. TITLE AND SUBTITLE
Advanced Distributed Learning Task 5(b)
Cybersecurity Barriers to Distributed Learning Modernization Report

5a. CONTRACT NUMBER
W911QY-16-C-0008

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0603769D8Z

6. AUTHOR(S)
Kathy Goodson, Ph.D.

5d. PROJECT NUMBER

5e. TASK NUMBER
5(b)

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Potomac Institute for Policy Studies
901 N. Stuart Street
Arlington, VA 22203

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Distributed Learnignf

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT
Distribution A. Unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
From interviews with the key subject matter experts, this report outlines the cybersecurity barriers to distributed learning modernization; including the investigation, validation, and documentation of the roadblocks created by cybersecurity policies and processes. This report reflects the examination of the opportunities and challenges associated with DL integration, and exploration of the related policies that may affect implementation new DL systems and applications systems. From interviews with key subject matter experts, the following themes were identified: 1) the broad application of cybersecurity policies geared toward standardized information technology security controls; 2) the difficulty in understanding and employment of current information technology cybersecurity policies and procedures to educational technology, and 3) the challenge between the desire to maximize information security from those that control the security side and maximize student accessibility from the education side.

15. SUBJECT TERMS
Distributed Learning, Cybersecurity, Information Assurance, Information Technology

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT (U)	b. ABSTRACT (U)	c. THIS PAGE (U)	None	85	Dr. Sae Schatz
					19b. TELEPONE NUMBER (*Include area code*) 407-208-5057

[Intentionally Left Blank]

Table of Contents

List of Abbreviations and Acronyms

ADL	Advanced Distributed Learning
ATC	Authority to Connect
ATO	Authority to Operate
CAC	Common Access Card
CIO	Chief Information Officers
DADLAC	Defense Advanced Distributed Learning Advisory Board
DL	Distributed Learning
DoD	Department of Defense
DoDI	Department of Defense Instruction
E-learning	Electronic Learning
ET	Educational Technology
FEDRAMP	Federal Risk and Authorization Management Program
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
IAM	Identity and Access Management
JKO	Joint Knowledge Online
LMS	Learning Management System
MGT	Modernizing Government Act
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PHI	Personal Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIPS	Potomac Institute for Policy Studies
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PNT	Positioning, Navigation and Timing
RMF	Risk Management Framework

Executive Summary

The Advanced Distributed Advanced Distributed Learning (ADL) Initiative asked the Potomac Institute for Policy Studies (PIPS) to conduct a study to identify cybersecurity distributed learning (DL) modernization barriers to understand the potential implications of promulgating the DoDI 1322.cm on costs, implementation, consequences, and gaps, and to develop implementation recommendations. The Potomac Institute conducted research to identify, determine the implications of, and recommend solution approaches associated with related policies that may affect implementation of DL in accordance with the updated DoDI 1322 policies. As part of this task, the Potomac Institute interviewed government stakeholders to identify DL roadblocks created by cybersecurity policies and processes within different Services (Army, Navy, Marine Corps, Air Force) and Organizations (Joint organizations/Joint Knowledge Online) are facing, and their approaches to addressing them.

From interviews with the key subject matter experts, this report outlines the cybersecurity barriers to distributed learning modernization; including the investigation, validation, and documentation of the roadblocks created by cybersecurity policies and processes. This report reflects the examination of the opportunities and challenges associated with DL integration, and exploration of the related policies that may affect implementation new DL systems and applications systems. From our interviews with the key subject matter experts, the following themes were identified:

- **The broad application of cybersecurity policies geared toward standardized information technology security controls.** Cybersecurity compliance of educational technology, systems and applications, are directed by guidelines and controls set in place by information technology standards without the incorporation of evolving distributed learning needs. As a result, there are incompatibilities in both cybersecurity policies and compliance timings as applied to distributed learning technologies.

- **The difficulty in understanding and employment of current information technology cybersecurity policies and procedures to educational technology**. Application of current cybersecurity policies to distributed learning technologies places limits on the identity management and authentication tools needed for anywhere, anytime learning.

- **The challenge between the desire to maximize information security from those that control the security side and maximize student accessibility from the education side.** Distributed learning stakeholders use disparate information systems and technologies to meet the needs and cutting-edge course delivery model expectations of end users. There is an overall disconnect between achieving the best possible distributed learning end user experience, and implementation of cybersecurity policies and procedures.

The outlined cybersecurity modernization themes are not mutually exclusive, but are categorized to highlight specific areas of stakeholder concern. The report lists the prevalent distributed learning cybersecurity obstacles that many of the interviewed Service stakeholders are trying to overcome and is organized into a body and appendixes. The body of the report is intended to provide details on the cybersecurity distributed learning modernization themes described above, and additionally cite solution approach areas for potential return on investment. The appendices of the report provide the supporting data and detail that substantiate the discussion presented in the body. These include: Appendix I: Task

5(b) Procedures and Structured Approach, Appendix II: Coding and Analysis, and Appendix III: Stakeholder Interview Data.

Introduction

The DoD is making a concerted effort to address Information Technology (IT) modernization in order to increase mission effectiveness, improve interoperability, and deliver capabilities faster.[1] This is a focused shift from the previous decade of federal government IT spending (**Figure 1**: **2010 - 2017 Federal IT Investment**). Current IT modernization efforts include attention to the consolidation of networks, the strengthening of information technology investments including a focus on cybersecurity, and development of an information technology workforce.[2] Potential Information Technology areas to be addressed by DoD modernization efforts include mobile end user devices (smart phones), networks, (unclassified and classified networks; wireless networks) services (cloud-based services), systems (system interfaces, and associated training/testing/maintenance support systems) and applications (web based applications; position, navigation, and timing (PNT) applications (i.e., GPS)).[3]

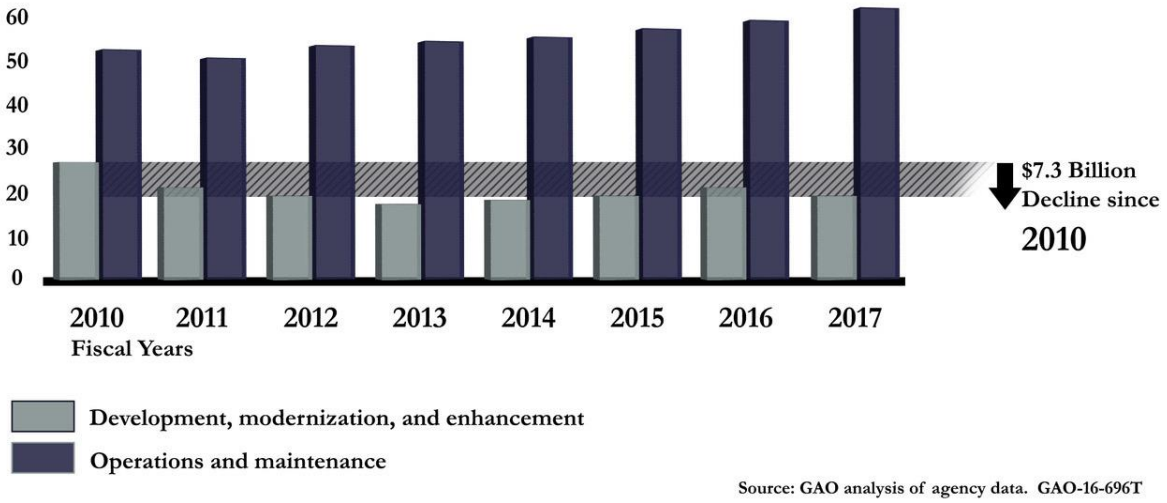

Figure 1: 2010 – 2017 Federal IT Investment Government information technology (IT) investment in the last decade has been geared toward operations and maintenance (O&M). In past few fiscal years, there has been an increase in the funding towards related O&M activities, and not in areas such as IT modernization.[4]

The Modernizing Government Technology Act (MGT) gives agencies additional resources to support movement to the cloud, and implementation and integration of shared services.[5] Within the next three

[1]Department of Defense Information Enterprise Strategic Plan 2010-2012. https://DoDcio.defense.gov/Portals/0/Documents/DoDIESP-r16.pdf
[2] Report to the President on Federal IT Modernization. 2017. https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf
Takai, Teri. 2012, Jan 05. DoD CIO's 10-Point Plan to IT Modernizationhttps://DoDcio.defense.gov/Portals/0/Documents/ITMod/CIO_10_Point_Plan_for_IT_Modernization.pdf
[3] DoD CIO. 2017, November 03. DoD Instruction 8420.01 Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DoDi/842001_DoDi_2017.pdf?ver=2017-11-03-092912-313
O'Neal, Matthew R; Dixon, Joshua S; 2011, June. Department of Defense Strategic and Business Case Analyses for Commercial Products in Secure Mobile Computing. http://www.dtic.mil/dtic/tr/fulltext/u2/a547816.pdf
[4] Powner, David A. 2016, May 25. Information Technology: Federal Agencies Need To Address Aging Legacy Systems U.S. Office https://www.gao.gov/assets/680/677454.pdf
[5] H. Rept. 115-129 - MODERNIZING GOVERNMENT TECHNOLOGY ACT OF 2017. https://www.congress.gov/congressional-report/115th-congress/house-report/129/1

years, more that 3 billion dollars' worth of federal government operational information technology equipment will become obsolete.[6] There is a high demand for new technology; however, processes for cybersecurity compliance needed for current distributed learning technologies and cybersecurity considerations for the acquisition of new distributed learning resources slow the pace of modernization. DoD stakeholders are prescribed into intransigent, policy fixed existing systems and consider the cost and time to transition towards implementations of distributed learning modernization a significant obstacle.

DoD cybersecurity requirements account for a 12-14 percent price gap between commercial and DoD products.[7] The median expenditure to complete the FedRAMP (Federal Risk and Authorization Management Program) process is 2.3 million dollars, not including the additional 1 million dollar annual expenditure for continued monitoring required for management and sustainment.[8] Additionally, it can take 18-24 months, which is approximately an information technology "generation" for such processes; in such cases, these requirements result in DoD systems being at least a generation behind when they are fielded.[9] This circumstance makes it difficult for DoD Services and Organizations to maintain cutting-edge technologies and the associated learning resources.

In order to move toward technological and educational innovations, the military has set forth[10] cybersecurity challenges as related to distributed learning that must be addressed. Government distributed learning stakeholders were interviewed to identify opportunities and challenges associated with (1) DL modernization as related to cybersecurity, and (2) navigating cybersecurity processes and procedures through the implementation of new DL systems and applications. Specific insights were gathered from education and training commands related to barriers in getting new systems the authority to connect/authority to operate (ATC/ATO) within cybersecurity processes. Though the stakeholders approached the topic from different perspectives, multiple common themes were identified, including, (1) the broad application of cybersecurity policies geared toward standardized information technology security controls, (2) the difficulty in understanding and application of current information technology cybersecurity policies and procedures to educational technology, and (3) the challenge between the desire to maximize information security from those that control the security side and maximize student accessibility from the education side. The details from stakeholder perspective are outlined and discussed in the following sections of this report.

---

[6] Conger M. 2017, October 02. Making sense of the IT modernization challenge. https://fcw.com/articles/2017/10/02/comment-it-modernization.aspx

[7] U.S. Government Accountability Office. 2017, July 20. MILITARY ACQUISITIONS: DoD Is Taking Steps to Address Challenges Faced by Certain Companies
GAO-17-644: https://www.gao.gov/assets/690/686012.pdf

[8] Ware, Tony. 2016, September 12. Average FedRAMP authorization costs $2.25M.
https://www.federaltimes.com/smr/acquisition/2016/09/12/average-fedramp-authorization-costs-2-25m/
Valdes, Jeff. 2018, July 10. The True Costs of Self Compliance for SLED Organizations. https://blog.rackspace.com/the-true-costs-of-self-compliance-for-sled-organizations

[9] Acquisition Reform to Enable Military Effectiveness. (2017, November 08). Retrieved from http://cpppe.umd.edu/publications/acquisition-reform-enable-military-effectiveness; Gansler, Jacques; Lucyshyn, William. 2012, July 01. "IT Acquisition: Expediting The Process To Deliver Business Capabilities To The DoD Enterprise." cpppe.umd.edu/publications/it-acquisition-expediting-process-deliver-business-capabilities-DoD-enterprise.

[10] Trump, Donald. 2017, December. National Security Strategy of the United States of America. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf 2018 National Defense Strategy; Mattis, James N. 2018, January 19. Summary of the 2018 National Defense Strategy of the United States of America Sharpening the American Military's Competitive Edge. https://DoD.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Broad Application of Cybersecurity IT Policies to DL

The broad application of cybersecurity policies geared toward standardized information technology security controls.

Cybersecurity policies and processes make navigating the implementation of any new distributed learning systems used within the government, DoD, and military education and training organizations a unique challenge as it must consider multiple high-level systems containing multi source software applications, and that are all interconnected and accessed by tens of thousands of various users on a daily basis. Current DoD cybersecurity policy[11], as mitigated by the NIST Risk Management Framework (RMF) [12], and standards[13] focus more on a system level management and compliance approach[14]; however, funding for cybersecurity implementations, including modernization often take more of a program level process approach as it is recurrently linked to acquisition cycles.[15] Ultimately, the management of distributed learning cybersecurity vulnerabilities crosses system and program level boundaries[16], leading to both policy incompatibilities and compliance timing incompatibilities. Addressing current cybersecurity policies and procedures, and meeting the needs of distributed learning has led to the following challenges:

- **The assumption that military education technology is a subset of information technology**[17] **is part of the problem and challenge.**[18] Historically, cybersecurity management processes, procedures, and security controls have been developed with a focus on information technology systems and not military systems.[19] This situation is further complicated when you take into account the specific expectations of military distributed learning technologies – they must close the gap between physical space limitations and providing tailored educational instruction to decentralized Warfighters[20]. Hence, related cybersecurity challenge solutions are not well suited to meet the evolving needs for military distributed learning technologies. Cybersecurity procedures and processes that take into

[11] Department of Defense INSTRUCTION NUMBER 8500.01. 2012, March 14. www.esd.whs.mil/Portals/54/Documents/DD/issuances/DoDi/850001_2014.pdf

[12] Joint Task Force. 2018, May. Risk Management Framework for Information Systems and Organizations. csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-draft-ipd-with-line-nums.pdf.

[13] National Institute of Standards and Technology (NIST). 2011, March. SP 800- 39 Managing Information Security Risk: Organization, Mission, and Information System View. https://csrc.nist.gov/publications/detail/sp/800-39/final

[14] DoD Instruction 8510.01. 2014, March 12. Risk Management Framework (RMF) for DoD Information Technology (IT), p. 10. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DoDi/851001_2014.pdf

[15] Snyder, Don; Powers, James D; Bodine-Baron, Elizabeth; Fox, Bernard; Kendrick, Lauren; Powell,Michael H. 2014, September 09. Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf

[16] Clark, Mark A; Espinosa, J. Alberto; Butina, Mariia. 2018, March. https://www.american.edu/kogod/research/cybergov/upload/CybersecurityKnowlNetworks_Mar2018.pdf

[17] Information Technology [40 U.S.C., Sec. 1401]: *Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.*

[18] Barrett, Matt; Marron, Jeff; Yan Pillitteri, Victoria; Boyens, Jon; Witte, Greg; Feldman, Larry. The Cybersecurity Framework Implementation Guidance for Federal Agencies. 2017, May. https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

[19] Snyder, Don; Powers, James D; Bodine-Baron, Elizabeth; Fox, Bernard; Kendrick, Lauren; Powell, Michael H. 2014, September 09. Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf

[20] Davis, Richard A. 2017, April 13. The US Army Learning Concept for Training and Education 2020-2040. adminpubs.tradoc.army.mil/pamphlets/TP525-8-2.pdf; Roberson, D. L., & Stafford, M. C. (2017). *The redesigned Air Force continuum of learning: Rethinking force development for the future*. Maxwell Air Force Base, Alabama: Air University Press, Curtis E. LeMay Center for Doctrine Development and Education.

account multiple approaches to information technology and education technology, potentially addressing specific distributed learning configuration guidelines for risk mitigation, will be required to better ensure more efficient and effective, reliable and secure distributed learning services. [21]

- **DoD information technology management, oversight, and budgeting is rigidly program based for compliance.** Distributed learning technology stakeholders are heavily constrained into [annual] program budgeting cycles when it comes to acquiring (and developing) human capital cybersecurity resources, and meeting DoD standards for cybersecurity system design requirements. Because information technology threats and technology itself are both continuously evolving, users are always aware of the potentiality for IT/ET systems to compromise defense measures throughout the entire life cycle of distributed learning technology products.[22] An organization's security procedures, and access to resources, must therefore be able to both adapt and respond as fluidly as cross program potential of a cybersecurity vulnerability.

Employment of IT Cybersecurity Policies and Procedures to ET

The difficulty in understanding and employment of current information technology cybersecurity policies and procedures applied to educational technology.

Cybersecurity barriers to distributed learning modernization involve the use, the application and the magnitude of the policies surrounding public key infrastructure (PKI). [23] The base of distributed learning users requiring Personal Identity Verification (PIV)[24] as provided through Common Access Card (CAC) technology for authentication on DoD networks is huge, and continuing to grow.[25] The current and future landscape of military distributed learning environment must take into account (1) the (physical) constraints of military tactical environments – i.e., bandwidth and networks, and (2) enabling any location, any device authentication. Distributed learning stakeholders outlined the following challenges in these areas:

- **New authentication processes will be required in order to access information especially when that information is levied by PKI and CAC tool sets.** The DoD has implemented their own unique infrastructure to satisfy operational needs; the exchange of data between users and technology is facilitated by PKI. PKI encompasses the hardware/software, human capital, policies/procedures used to facilitate, identify, and manage the secure exchange of information via networks (i.e., internet, email), and employs hardware/software services that generate and manage encryption keys.[26] Current DoD encryption requirements utilizes two – factor authentication, with the most common

[21] Information Technology Chart 16-1. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_16_it.pdf
[22] National Conference of State Legislatures. Budgeting for Cybersecurity.
http://www.ncsl.org/documents/taskforces/Budgeting_For_Cybersecurity_32041.pdf
[23] NENA Next Generation 9-1-1 Security (NG-SEC) Information Document. 2016, December.
https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-INF-015_NGSEC_INF_20161.pdf
[24] NIST 800–157 — Guidelines for Derived Credentials https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-157.pdf;https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD%20CIO%20CS%20Reference%20and%20Resource%20Guide%202018_v9.1_Final_2018.pdf?ver=2018-08-23-103824-243
[25] FIPS 201-2. August 2013. Personal Identity Verification of Federal Employees and Contractors.
https://csrc.nist.gov/publications/detail/fips/201/2/final
[26] PKI stipulates encryption capability, providing the tools for compliance with DoD encryption requirements. NENA Next Generation 9-1-1 Security (NG-SEC) Information Document. 2016, December 08. https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-INF-015_NGSEC_INF_20161.pdf

access credentials being the CAC[27] and a Personal Identification Number (PIN).[28] The CAC possess integrated PKI certificates, and there are currently 1.5 million daily logged CAC transactions.[29] These certificates provide user identification and verification in real-time during distributed learning sessions.[30] Current DoD cybersecurity compliance standards as related to PIV prohibit mobile derived credentialing for authentication (assured identify) on secondary platforms.[31] Hence, with identity and access management (IAM) as related to PKI at the crux of the distributed learning cybersecurity compliance policies, there are several mitigating issues to overcome in terms of both policies for assured authentication and volume of end users that need authentication.

- **Stakeholders agreed that data storage and encryption must also be considered for organizations that house large amounts of Personally Identifiable Information (PII) and Personal Health Information (PHI).** Data storage considerations must take into account requisite values of the provided information, what constitutes both PII and PHI information.[32] Once the value of the information has been categorized an organization will be able to determine what needs to be preserved and protected and what needs to be permanently discarded thus reducing the costs required to store the information. Stakeholders felt that the full scope of the IT resourcing for PHI and PII were not taken into full consideration when their individual organization selected their cloud service provider and is one of the reasons they are hesitant to transition. Stakeholders believe that any organization considering transitioning to cloud computing must recognize that the processes involved in procuring and evaluating cloud services can be complex and must be evaluated and met prior to signing up. In short, any IT service holding and processing such data and information must be fit for purpose and meet business requirements. When individual organizations consider moving from their current data management to cloud platforms, considerations for both the non-functional and functional dimensions should be weighted across the organization.

- **Understanding how DoD cloud computing will continue to transform the way distributed learning stakeholders use, store, and share data; and ultimately consume IT resources.** Cloud computing allows pervasive, expedient, and on-demand network access to a collaborative consumption of configurable computational resources.[33] Cloud computing allows for increased efficiency, faster services at lower costs, plus improved business flexibility while simultaneously providing improved security. Yet there are several reasons why some organizations have not embraced the movement to

[27] The CAC card was developed in 2001 as identity management tool and remains the industry standard identification tool for Active duty and DoD civilian employees who regularly access defense computer networks and/or regularly access secure buildings and controlled spaces. Herrmann, Colleen M. 2001, July-September. Common Access Card: Security and Privacy. http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=3668 2.8 million CACs in 2015 and over 20 million over the last 15 years. Miller, Jason. 2016, June 15. DoD plans to bring CAC cards to an end. https://federalnewsradio.com/defense/2016/06/DoD-plans-bring-cac-cards-end/

[28] Muck, Steve; Daughety, Steve. 2012, July-September. The DoD Identification Number as PII. www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=4034.

[29] Gemalto. 2018, February 19. Military CAC: The United States Department of Defense DoD Common Access Card. https://www.gemalto.com/govt/customer-cases/usa-DoD

[30] Khouri, A. M. (2011). PKI in Government Identity Management Systems. *International Journal of Network Security & Its Applications,3*(3), 69-96. doi:10.5121/ijnsa.2011.3306

[31] Serbu, J. (2018, July 27). One alternative to the CAC: DoD will identify you based on your walking behavior. Retrieved from https://federalnewsradio.com/defense-main/2018/06/one-alternative-to-the-cac-DoD-will-identify-you-based-on-your-walking-behavior/

[32] The appendix of OMB M-10-23 "defines PII as information that can distinguish or trace an individual's identity alone or with other information that can be linked to a specific individual. This directive provides how to properly handle PII if a breach should occur.[32] The Health Insurance Portability and Accountability Act (HIPAA) defines PHI as information in a medical record that can be used to distinguish an individual and was created, used or disclosed for health care service. Orszag Peter R. 2010 June 25. Guidance for Agency Use of Third-Party Websites and Applications M-10-23. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf; USA, Department of Homeland Security, DHS Privacy Office. (2017). *Privacy Incident Handling Guidance*. DHS Privacy Office. https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017.pdf

[33] Mell, P., & Grance, T. (2011, September). SP 800-145, The NIST Definition of Cloud Computing. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-145/final

cloud computing even with the aforementioned benefits. Stakeholders cited a reluctance to move critical assets to the cloud because of increased security concerns and rigid technology acquisition practices. Distributed learning stakeholder concerns included that they may find they have less control over the function and execution of services within a cloud-hosted environment. While, they may retain control of proprietary software, applications, both stored and shared data, and proffered services, they may not retain the level of control previously held when it comes to backend user infrastructures such as security. Stakeholders agree, as with any infrastructure service, that the suitability of cloud-computing for an organization's specific use case should be assessed prior to transition via thorough risk-based analysis, validation and verification: these processes require resourcing. Overcoming these cybersecurity and acquisition positions will require the right combination of people, processes and technology to mitigate risk and substantiate the cloud's inherent efficacy.

Challenge of Maximizing Security and Accessibility

Challenge between the desire to maximize information security from those that control the security side and maximize accessibility from the education side.

Currently, distributed learning stakeholders are forced to explore the use of disparate information systems and technologies, and information delivery models that meet the needs and expectations of end users. Distributed learning training and education models offer significant student engagement via an online educational Learning Management System (LMS) tailored to any given institution's mission and goals.[34] Modern LMS' employ software applications that will deploy and track online training initiatives as well as cognitive learning improvements.[35] Cybersecurity compliance is further complicated by distributed learning environments that must maintain the coexistence of distributed learning legacy hardware and modern applications. Distributed learning stakeholders outlined the following challenges in these areas:

- **According to stakeholders one of the most important shared challenges is that current systems rely on a mix of legacy and modernized technology to support programs and daily operations.** While it may be less complicated in the current technological environment to deploy and monitor security updates and features for newly deployed systems, it is a practicality that vendors will eventually stop supporting legacy systems making them [even more] susceptible to security vulnerabilities.[36] Once an attacker identifies a legacy system, it invariably becomes a target. Distributed learning organizations may draw from training and education content from interconnected web nodes from other organizations. However, organizations have no control over the frequency of cybersecurity compliance system processes, software security update schedules, of other organizations. This leads to overall variability in content access, interrupting daily distributed learning function needs. The scale and complexity of this problem makes security updates one of the most important challenges when it comes to protecting large groups of digital environments.

[34] Wright, Clayton; Lopes, Valerie; Montgomerie, Reju Sunday; Schmoller, Seb. 2014, April 21. Selecting a Learning Management System: Advice from an Academic Perspective. er.educause.edu/articles/2014/4/selecting-a-learning-management-system-advice-from-an-academic-perspective.
[35] Ibid.
[36] Kozlowicz, J. (2018, May 4). Legacy Systems Remain Because They Work - But They Could Be a Major Security Risk. Retrieved from https://www.greenhousedata.com/blog/legacy-systems-remain-because-they-work-but-they-could-be-a-major-security

- **Improving LMS performance, efficiency and service delivery are difficult when having to consider cybersecurity compliance for legacy hardware and modern software.** Currently, organizations are hindered in cybersecurity modernization because of by their need to adapt to varying policy and procedures to ensure that controls are in place to maintain a viable security posture between hardware and software.[37] Organizations may have access to an enterprise information technology services that will allow for the best possible user experience; however, they may not be able to modernize because the enterprise service does not meet the hardware encryption system requirements for cybersecurity compliance.

- **The cost of making software adaptations for achieving anywhere, anytime learning.** Training can now be delivered on multiple devices such as tablets, computers, and smartphones etc. Because of the widespread availability of these devices, course curriculums can potentially be delivered anywhere anytime. However, resources for adapting software to meet the compliance requirements related to particular specifications for distributed learning hardware technologies are limited or nonexistent. In some cases, contract modifications may be necessary for implementing changes.

Conclusion

Through efforts that will focus on the infrastructure of information technology networks and strengthening of processes for cybersecurity technology investments, the DoD is working towards performance improvements that will deliver capabilities faster and more efficiently, and at the same time promote interoperability. Within this environment, distributed learning stakeholders are navigating DoD cybersecurity approval processes with the implementation of new DL systems and applications. Through our exploring distributed learning (DL) modernization best practices related to cybersecurity, we determined the opportunities and challenges associated with DL integration, and potential solution approaches associated that may affect implementation of DL.

Although distributed learning stakeholders consider cybersecurity challenges from very unique perspectives, the broad application of cybersecurity policies geared toward standardized information technology security controls, the difficulty in understanding and employment of current information technology cybersecurity policies and procedures to educational technology, and the challenge between the desire to maximize information security from those that control the security side and maximize student accessibility from the education side, are underling themes that are shared amongst the stakeholders.

From our cybersecurity policy and process discussions with distributed learning stakeholders from the Services (Army, Navy, Marine Corps, Air Force) and Organizations (Joint organizations/Joint Knowledge Online) the following challenges were identified:

- **The assumption that military education technology is a subset of information technology is part of the problem and challenge.** The challenges and risks surrounding cybersecurity management processes, procedures, and security controls have been created with a focus on information technology systems. Therefore, military systems are continuously left wanting with respect to cybersecurity solutions

[37] IES National Center for Education Statistics. Part 6: Maintaining and Supporting Your Technology. nces.ed.gov/pubs2005/tech_suite/part_6.asp.

- **DoD information technology management, oversight, and budgeting is rigidly program based for compliance.** Distributed learning technology stakeholders are heavily constrained by annual program budgeting cycles. When it comes to acquiring human capital cybersecurity resources and meeting DoD standards for cybersecurity system design requirements the stakeholders have a difficult time adapting to new advancements in technology and/or processes.

- **New authentication processes will be required in order to access information especially when that information is levied by PKI and CAC tool sets.** Evolving demands for distributed learning needs will require addressing new authentication practices.

- **Stakeholders agreed that data storage and encryption must also be considered crucial for organizations that house large amounts of Personally Identifiable Information (PII) and Personal Health Information (PHI).** With adversarial threats evolving on a daily basis, the DoD must continuously evaluate

- **Understanding how DoD cloud computing will continue to transform the way distributed learning stakeholders use, store, and share data; and ultimately consume IT resources.** The components required to achieve sound organizational security and sustained cloud technological governance will be a challenge that will require ongoing attention.

- **According to stakeholders one of the most important shared challenges is that current systems rely on a mix of legacy and modernized technology to support programs and daily operations.** The scale and complexity of having both legacy and modern technology creates a situation where security updates that protect large groups of digital environments becomes a primary stakeholder challenge.

- **Improving LMS performance, efficiency and service delivery are difficult when having to consider cybersecurity compliance for legacy hardware and modern software.** Organizational compliance policies and procedures must ensure that effective controls are in place in order to maintain a viable security software/hardware posture to meet evolving distributed learning technology needs.

- **The cost of making software adaptations for achieving anywhere, anytime learning.** Facilitation, delivery, and management of multiple cyber compliant distributed learning offerings is significant hurdle for distributed learning organizations.

Although cybersecurity compliance policy are not intended to impede innovation, policy that focuses on risk aversion vs. risk assessment may hinder, and sometimes prevent completion of compliance processes. Within this context the type of solution approaches to these distributed learning cybersecurity concern areas will be those that address the policies that enable identity management and authentication, and the acquisition of cybersecurity complacent systems and services[38].

The application of current cybersecurity policies related to distributed learning technologies, such as the use of CAC authentication, places limits on the identity management and authentication tools necessary for anywhere, anytime learning. New technologies (biometric access, automation through real-time alerts and notifications) are transforming user authentication mechanisms. Microsoft has employed biometric technology to two-thirds of its employees with a simple authentication method with PIN backup balancing

[38] Advanced Distributed Learning Task 6 Acquisition for New Distributed Learning Report

usability with security[39] and Google is working on a password technology that measures multiple factors using "trust scores" that uses various data points such as the user's voice and facial features to determine whether or not they are legitimate.[40] Further research on DOD mobile derived credentialing options, in collaboration with further research government assured identity policies are areas for further study.[41]

Cybersecurity compliance of educational technology, systems and applications must be aligned to an organization's functional requirements and assurance necessities in relation to an organization's networking environment. DL stakeholders mentioned unique requirements in terms the types of projects that require computationally intensive processes to complete a task, the amount and type of data generated, and sensitivity of the data being handled. IT resourcing policy considerations, including information technology as a Service, for distributed learning stakeholder cloud environment needs is an area of further study.

There is an overarching challenge between Information security and accessibility. Organizations need to maximize accessibility in order to allow end users access to necessary information systems, and related tools and applications required to complete tasks from decentralized locations in operational environments that include legacy systems. One of the ways to bridge the disconnect between achieving the best possible distributed learning experience and the implementation of cybersecurity guidelines further investment in looking into the legislative and acquisition policies regarding the IT posture of legacy systems. NIST has recently provided guidelines for the cyber resiliency of legacy systems.[42] The application and resulting implications of these guidelines to DL legacy systems would be an area of further study.

Updates to technology policy standards should address areas concerning identity management and authentication, assured identity, and the determination of security controls and protocols for distributed learning technologies. Efforts that bridge the gap of DoD agencies and distributed learning organizations, specifically in the areas ATO are a direct asset toward resolving some of the cybersecurity roadblocks discussed in this report. [43] Additionally, platforms[44] for distributed learning stakeholders to directly share with each other the impact of meeting cybersecurity policy compliance within their system and application implementations, and direct distributed learning case studies for successfully completed processes would be value added.[45]

[39] Ford, Robert. 2018, Sept 2018. No more passwords: the relentless commitment to creating a password-less world at Microsoft. https://www.microsoft.com/itshowcase/blog/no-more-passwords-the-relentless-commitment-to-creating-a-password-less-world-at-microsoft/

[40] Biometrics: From Fingerprints to the New Frontier. (2018, March 22). Retrieved from http://now.northropgrumman.com/biometrics-from-fingerprints-to-new-frontiers/

[41] https://disa.mil/NewsandEvents/2018/DOD-identity-access-management-cap

[42] Goldstein, P. (2018, April). How Feds Can Secure Legacy IT Systems. Retrieved from https://fedtechmagazine.com/article/2018/04/how-feds-can-secure-legacy-it-systems; Joint Task Force. (2018, October). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (Publication No. SP 800-37 Rev. 2). Retrieved from NIST at https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft

[43] 18F is an office in the GSA that provides a technical project management support. 18F provides a number of informative "how-to's" and tutorials on topics related to government requirements around digital processes such as Authority to Connect and how to reduce the time spent on these efforts. https://18f.gsa.gov/

[44] Williams, Lauren C. 2018, May 25. Army focused on risk management framework. https://defensesystems.com/articles/2018/05/30/army-rmf-cyber.aspx

[45] Keller, N. 2018, April 12. Success Stories-Purpose and Benefits. https://www.nist.gov/cyberframework/success-stories

Appendix I: Task 5(b) Procedures and Structured Approach

Method and Design

For the types of issues, we expect to encounter with both tasks, it is not possible to fully anticipate the breadth or depth of issues that we will encounter. It is imperative, however, to have a structured approach and apply it consistently to the extent necessary to dive as deeply as necessary to get at *root causes*. For this method, we define *root causes* as those for which *actionable, implementable recommendations* can be made. This process of heuristic analysis, then, may require multiple analytic cycles to "peel the onion" of complex issues from what is often stated as the issue in reality being the effect, not the cause. Thus, participants are likely to define an issue in terms of its effect (the "what") rather than its cause (the how and why). Even for those who attempt to identify causes, those things they are calling causes are in fact the effects of deeper causes. Because we cannot identify, a priori, what the issues are going to be, we cannot lay out how many levels down we will need to dig to identify the root causes that result in higher-level effects.

Overall Approach

Potomac Institute for Policy Studies (PIPS) will draw from our interviews with the key subject matter experts the most prominent obstacles that many/all the Services are trying to overcome. PIPS will then analyze to explore core causes and address specific recommendations ADL may employ (policy update, technology demonstrator, changes to procedures etc.) to address the problems. Questions are developed to (a) identify the particular problems within different Services (Army, Navy, Marine Corps, Air Force) and Organizations (Joint organizations/Joint Knowledge Online) are facing and (b) their approaches to addressing them.

The study will be based upon participant responses to predetermined semi-structured open-ended questions. The experimental materials include an interview script.

Population of subjects to be studied

PIPS has identified the updated DoDI 1322.26 stakeholders, DL Cybersecurity Technology Stakeholders, and Service POCs for the ADL Initiative, Defense ADL Advisory Committee (DADLAC). These groups will be recruited to participate in this study and will be asked to identify additional related DoD distributed learning stakeholders for interviews. All participants will be 18 years or older.

Inclusion/exclusion criteria

PIPS Research Associates, in conjunction with ADL, will compile a list of qualified subject-matter-experts (SMEs) with experience in DL modernization, implementation, and integration issues.

Safeguards

Privacy and confidentiality: All interviews will be not for attribution. Audio recordings are prohibited during these meetings. Written notes will be coded and stored with numeric experimental identifiers. The master list of the coded and stored numeric experimental identifiers will be kept under lock and key with access restricted to the study lead.

Risk/Benefit - Data Safety and Monitoring Plan

The study poses minimal or transitory risk. For example, responding to questionnaires or feeling embarrassment about an organization's ability to acquire DL systems. There are indirect benefits for participation in the study. For example, a sense of pride in contributing to the knowledgebase, and potential for future improvements on cybersecurity/acquisition processes. Interactions includes the following interactions between investigator and SME: face-to-face and phone interaction with questionnaires and laptop computer.

The study will be reviewed and governed by PIPS investigators, including the Principal Investigator, Kathy Goodson, Subject-Matter-Expert, Thomas O'Leary, Subject-Matter-Expert, Laura Worcester, Subject-Matter-Expert, Dwight Lyons, Research Associate, Adam Steele and Research Associate, Sabrina Worcester. Collected information and data will be delivered to ADL at the end of the contract period. Back up collected information and data will be destroyed by PIPS at the end of the contract period. Adverse events are not anticipated. The PIPS investigators are responsible for review of cumulative adverse events which will be documented and reported accordance to the policies and procedures of the Human Research Protection Program (HRPP).

Recruitment

Identified SMEs for the Cybersecurity Barriers to Distributed Learning Modernization and Acquisition for New Distributed Learning will be contacted by PIPS to discuss the study parameters and set up potential interview dates. This includes members of the PIPS cybersecurity, acquisition, and policy SME network. Participants may choose not to participate at any time**.** We anticipate that SMEs contacted first may not have all the information needed to conduct the multiple cycles needed to get from top-level effects to underlying root causes. Thus, we expect that initial interviews will identify additional types of personnel that need to be contacted to pull the threads from effect all the way through to root cause(s).

Potential initial SMEs to include:

Acquisition and Requirements POCs

- Chief Information Officers (CIOs)
- Authorizing Officials (AOs)
- DISA Infrastructure Engineering (IE) POCs

DL Cybersecurity Technology Stakeholders

- DL technical designers
- JKO technologists (hardware/software developers)

DL Service POCs

- DADLAC
- Military Education POCs

Demographics

1. Active, Reserve, Civilian

2. Position/Organization

3. Title/Rank

4. Experience with DL systems

5. Experience with DL modernization efforts/Experience with DOD acquisition process

Tasks 5(b) Procedures to be followed

Task 5 (b) Semi-Structured Interviews

Interviews will take place via telecom or in person with individual stakeholders. There will be a general series of initial semi-structured open-ended questions. Based on stakeholder responses, follow on questions may be asked to further the discussion. PIPS will request stakeholders allow 30-45 minutes but no longer than 60 minutes.

1. Stakeholders will meet with 1 facilitator and 1-2 rapporteurs.

2. Stakeholders will be asked to respond to interview questions in order to further project discussion.

3. Upon completion of the interview, researchers will request follow-up dates and times with the stakeholders via phone or email if additional information is required.

Task 5b Research Apparatus

The research apparatus will consist of the following sections.

1. Semi-structured open-ended questions, for the purpose of elaboration of identified barriers.

2. Statements related to the perception of Cybersecurity Barriers to Distributed Learning Modernization, utilizing a Likert scale analysis ranking system

Statements from the semi-structured open-ended questions will describe known barriers and stakeholders will be asked to rank these in order of impact. Barrier categories will be broadly classified around the individual themes identified. Stakeholders will be asked to rank their perceptions of the impact of selected barriers on their ability to modernize distributed learning with the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact.

Data Analysis

1. Responses to the open-ended questions will be summarized qualitatively and quantitatively examined for themes, specific data, and other information.

2. Responses to the Likert scale analysis ranking system will be further analyzed in order of impact or need.

Task 5(b) Semi Structured Interview Questions

Final goal: Task 5b - Identify the opportunities and challenges associated with DL integration and provide (specific actionable) potential solution approaches associated with related policies that may affect implementation of DL.

Intro Script Task 5b

- The Potomac Institute for Policy Studies (an independent, 501(c)(3), not-for-profit public policy research institute in Arlington, VA) is supporting the Advanced Distributed Learning Initiative (ADL) in a task to explore distributed learning (DL) modernization best practices.
- As part of our task, we are interviewing government stakeholders to identify the opportunities and challenges associated with DL modernization.
- These interviews will directly inform our research on identifying potential pathways to address the challenges of DL modernization related to cybersecurity.
- This research aims to identify root causes that lead to barriers in getting new systems the authority to connect/authority to operate (ATC/ATO) within cybersecurity processes.
- We are interested in discussing the successes and barriers you and your organization have had with navigating the implementation of new DL systems and applications.
- Non-attribution Statement: All correspondence collected during interviews, surveys, or through other forms of information generation will be safeguarded by the research team. Without the express permission of the interviewee, nothing he or she says will be attributed to that speaker directly or indirectly and/or released to anyone who was not affiliated or involved with the information exchange. The research protocol will not involve names as identifiers and attribute data to an interviewee through a coded system. All research material is for the expressed purposes of the research team and members of ADL.
- The goal this research is to identify the opportunities and challenges associated with DL integration and provide actionable potential solution approaches associated with related policies that may affect implementation of DL.

Task 5(b) Interviews Overview

1. What are the current DL systems utilized by your organization and how are these systems being modernized?
2. Describe the DL cybersecurity processes related to upgrading and modernizing your organization's systems.
    a. How do/what DOD cybersecurity policies most effect these processes?

b. What internal cybersecurity protocols most effect these processes?

3. Comprehensively describe your organization's top cybersecurity barrier impacting modernization.
    a. Describe possible causes/root causes and their sources.
    b. Are the causes for the described cybersecurity barrier common to other DOD Services and Organizations?
    c. What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]?
    d. What one to three actions would most help overcome this barrier.
4. Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of:
    a. Manning
    b. Training
    c. Equipping
5. Describe how DL cybersecurity policy impacts decision-making process with regards to:
    a. Hardware
    b. Software
    c. Networks
    d. Cost
6. Describe your organization's cybersecurity compliance process as related to movement to cloud services?
    - How important is it that cloud services are standardized?
7. Within your organization's procedures for obtaining authority to operate/authority to connect (ATO/ATC), are there specific issues that are causing the most difficult delays/cost incurrences?
8. What are some areas related to the issue(s) just discussed where you think the ADL Initiative can help your organization?

Appendix II: Analysis and Coding

Pre-set and emergent codes that were assigned to the raw data that was collected during the stakeholder interviews.

Task 5b Cybersecurity Barriers to Distributed Learning Modernization – Identification Pre-Sets:

- Program costs
- Equipment and support (capital investment)
- Resource availability (personnel)
- Scheduling (delivery/planning)
- Technical (internet access)
- Instructional concerns (program development/professional development)
- Policy/procedural
- System/component description

Analysis Code:

- Category: ISSUE/BARRIER
    - Subcategory 1: Policy (POL)
        - Code: UPDATE-Identified areas for new and/or upgraded distributed learning technologies.
        - Code: APPLICATION-How the policy is applied to any given situation.
        - Code: INCOMPATIBILITIES-Incorporating disparate technologies that work homogeneously.
    - Subcategory 2: Technology (TECH)
        - Code: NEW ACQUSITION- Obtaining new SW/HW/Service
        - Code: UPDATE/INFORMATION- Obtaining different SW/HW/Service
        - Code: INSTRUCTION/DEMONSTRATION-Identified areas where there is a need to not only define what was needed and how solutions may be applied.
    - Subcategory 3: Procedural (PRO)
        - Code: INTERNAL PROCESS- The way in which an individual organization conducts business.
        - Code: EXTERNAL PROCESS-The way in which other organizations conducts business.
        - Code: TIMING-Timing differences between processes and procedures (i.e. annual assessment vs. quarterly assessment.
    - Subcategory 4: Resourcing (RES)
        - Code: HUMAN CAPITAL-Personnel needed to address stakeholder stated need.
        - Code: NEED – Stakeholder stated need.

Analysis and Coding Table[46]**:**

Question	Responses	Analyst 1 Identifiers		Analyst 2 Identifiers	Comments
		Code	Frequency	Code	
1.What are the current DL systems utilized by your organization and how are these systems being modernized?	022 - We run all of our programs/SW on unclassified edu networks. There are cost benefits of being on the edu. Example: we don't pay for office 365. Adobe gives us a better deal. (program costs)	TECH (UPDATE)	379	Tech	Requirement - Cost-effective, interoperable, secure, and easy to use.
	346 - The delivery systems that we use are dictated by the interactive multi-media types that we utilize. Our primary system LMS for CMI is web based, not designed in the cloud environment it's running in the cloud, it has a lot of moving pieces. (system/component description)	TECH (UPDATE)		Tech	Requirement - end users integrate converged services and tools.
	368 - SCORM engine for content delivery, Microsoft sequel the backside database and question mark reception for assessments and surveys. We also support online professional military education programs we previously had Blackboard. Moodle. (system/component description)	TECH (UPDATE)	379, 373	Tech instruct/demo	Current LMS components being modernized

[46] The Rows reflect extracted stakeholder feedback (coded with numeric experimental identifiers) from the outlined questions. The chart Columns include the analysis Code and the Frequency, which is a reference to another stakeholder which may have stated or eluded to similar information.

	373 - Inside the environment holds the servers for Joint knowledge online apps which would be traditionally called the LMS. We also have a bunch of components. (system/component description)	TECH		Tech	Current LMS components being modernized
	381 - One agency service offering is called MILCLOUD 2.0. That is a cloud hosting environment that is available to all DoD components for them to host their services. (system/component description)	TECH	362	Tech New Aqu.	Pay as you go vs. flat rate hosting model offered by DISA. (Cost Savings)
	026 - They contracted to buy a COTS product that would integrate a student mgmt. system and LMS and meet all the reqs of probably what was a dozen student mgmt. systems that existed. That contact did not execute well, we didn't get an integrated system. (system/component description/equipment and support (capital investment)	ISSUE/BARRIER - TECH (UPDATE), PRO	(380)	Pro. Internal Process	Example of contract complications where deliverable was not met. (Integration of LMS and SMS was not achieved) (acquisition implication)
	407-We are working on procuring an external portfolio tool that will replace what SAKAI is no longer going to support. (system/component description)	ISSUE/BARRIER - TECH (UPDATE)		ISSUE/BARRIER - TECH (UPDATE)	Factors that impact performance and user experience.
	405-Our modernization program is underway now, we are pilot 1 which means we procured Adobe Experience Manager to be a front facing tool that provides individualized learning to communities of interest. We are	TECH		Tech New Aqu.	Current LMS components being modernized

	working on integrating that with Moodle so that we are working towards creating a e-learning ecosystem for the XXXX. (system/component description)				
	362 -The reality is we haven't acquired much for a number of years, SAKAI has been our LMS for over 10yrs. We engaged a company within the SAKAI community that does customization for us so outside of that our work in the imperial community the only quasi learning tech tool that we've acquired was for lecture capture which we did last yr (system/component description)	TECH	373, 380	Tech Update/information	Org uses a free, community source, educational software platform designed to support teaching, research and collaboration. Updates to the platform can be downloaded from the company. (Cost savings)
2. What challenges from the cybersecurity perspective do you run into?	022 - You name the piece of HW/SW it won't be smooth. My experience with NMCI, it is locked down at such a level with the breadth of what we do. If we had to put the policy on every laptop, we have a large nonresident student pop, unlike the war college, do the reading and submit the exam via email. All of ours is synchronous delivery. We couldn't operate on the military networks with any kind of effectiveness. (policy/procedural)	ISSUE/BARRIER - POL (INCOMPATIBILITIES)		Pol Incompatibilities	Although cost effective and serves to support, current security restrictions are hindering.

	346 - The difficulty is while moving something to .edu it doesn't fix the problem because if your transit any part of the NIPRnet, systems like HBSS latch on to whatever's running across. 90% or more of all DL is taken on a govt computer in a govt workplace which is inside the NIPRnet. (policy/procedural)	ISSUE/BARRIER - POL, TECH, PRO	(380) 025	Pol. Update	Cybersecurity controls span across education and training environments.
	025 - How do they see service members accessing content for the next 2,4,6,10 yrs. There are ppl who say anytime anywhere and then you talk to cyber or PII ppl and they don't really understand. A lot of orgs are going to content anytime anywhere but if you can't get to it then what the use in having it? (policy/procedural)	ISSUE/BARRIER - POL ; TECH (INSTRUCTION/DEMONSTRATION)		Pol. Incompatibilities, Procedures Internal	Factors that impact access and how to resolve them
	368- the biggest thing we are facing is being one of the first lg orgs to leave a DoD enclave and move to amazon web services. The challenge there is getting ppl to understand that amazon web services is a secure environment. Because we are the first to do this on a lg scale, the challenge has been making sure controls are in place to maintain security posture. (policy/procedural)	ISSUE/BARRIER - PRO (TIMING/INTERNAL PROCESS)	(379, 346,)	Pro. Internal Process (ISSUE/BARRIER - POL)	Organization by in to new provider. (choice of particular system linked to cost and overall ease)

	362- It's a new fish bowl every time around. Our team will contact DISAs battle captain at FT Meade to say here is our issue what do we need to do in order to resolve? They end up sending a different form from before, we fill it out, it either gets lost or we'll need to resubmit with modifications or get someone's approval. We'll be required to cite regulatory authority and for the particular case of getting the website unblocked is a website that support secure digital certificate and that website is supposed to be trusted based on DISA provided systems that we are supposed to build our mobile computers off of.	ISSUE/BARRIER - PRO (EXTERNAL PROCESS)		Pol Incompatibilities	Problems navigating the ATO/ATC process
	405-We operate 2 networks (.mil and .edu) therefore, we somewhat side step challenges based on this. When someone asks if we are protecting the DoD network, we can say we don't touch the DoD NIPR.	PRO	362	PRO	Risk aversion vs. risk mitigation.
	373 - xAPI works well within our enclave but having a standardized approach on how you will track training across the services using this, how that all works is the key. Not necessary a cyber security issue it's understanding the information technology battlespace issue. (policy/procedural)	ISSUE/BARRIER - TECH (INSTRUCTION/DEMONSTRATION); POL (UPDATE)	025, 362	Tech instruct/demo	Interoperability. Understanding of system architecture.

	382 - we follow all the given policy guidelines for bringing a project into play. Whether it's standing up an app or full server there is a set of guidelines that is set up by the CA (certifying official) and certified by the AO (authorizing official). There is whole list starting with the NIST 80053, DoD reqs for RMF, STIG review of the apps so on and so forth. (policy/procedural)	ISSUE/BARRIER - PRO (EXTERNAL PROCESS)	348, 362	Pro. Internal	Reference to guidelines applicable to all individuals and organizations managing, or involved in, developing and/or implementing DL content and courseware.
	380 - As we talk about DoD and CIO has policy and we have to comply what we've seen over the past cpl of years is a small percentage of our time has to go towards implementing those policy changes that's all under the rubric of cyber security. Those types of services/compliances/frequency of policy changes are going to go up in the future. As XXX needs to manage he also has to keep an eye on how it's starting to increase the ratio of what we get done with our resources. (policy/procedural - resource availability)	ISSUE/BARRIER-POL (APPLICATION)		Pol. Application	Fungible reference.
	026 - From the cyber standpoint, the fact that we were driven to everything being FedRamp constrains the options you have available to you to solve these IT/ET challenges. (policy/procedural)	ISSUE/BARRIER-POL (APPLICATION)	362	Pro. External	IT compliance [classification] of systems and applications as related to education and training.

	362 - Background on environment- We have some advantage over some DoD orgs from an IT standpoint we operate 2 networks (.mil and .edu) We make some exceptions on our .edu commercial network. We have some capabilities along the DL lines that comes through acq over the yrs that I don't think we would have been able to do if we were 100% NIPR org. (policy/procedural)	ISSUE/BARRIER - POL (External)	026	Pro. Internal Process	Co-existing networks that allow for them to achieve their mission. (Have processes where they operate two different networks but still does not address the overall access issue.)
a. What do you think is the cause for the cybersecurity challenge your organization is facing?	026 - Number one thing-this blanket approach since we view everything in operational terms and were going to apply security reqs inherently constrains the options available, lengthens the timeline to get capabilities on and costs more money. (policy/procedural)	ISSUE/BARRIER - POL (INCOMPATIBILITIES)/Need	362	Pol. Incompatibilities, Procedures Internal/Need	The IT compliance approach will need to vary depending on the security risk factors for each capability (priority list).
	368 - Because we are the first to do this on a lg scale, the challenge has been making sure controls are in place to maintain security posture. (policy/procedural) (AWS)	ISSUE/BARRIER - PRO (INTERNAL PROCESS)		Pro. Internal Process	Maintaining IT organizations posture will require human capital investments, technologies, and processes.
	011 - What I'd like to see is an understanding of the DoD process for approving applications. What are the rules that DISA wants you to go by? Engage DISA early to find out what the standards are to be able to operative or would I be better off in my distance learning to go to a .edu network that is separate? As a leader, I'd want to know if that is a way to protect the DoD network. It will boil down to	ISSUE/BARRIER - PRO (INTERNAL PROCESS)	373, 381	Pro. Internal Process	Front end cybersecurity implications.

	being able to encrypt your information. When I look at modernization one of the things I'd like to know is "Is there a way of doing it that allows me to keep Personally sensitive information secure before becoming a burden or on security requirements that need to build into it? Is there a way I can do that? (policy/procedural)				
b. How do/what DoD cybersecurity policies most effect these challenges?	025 - I think that goes back to risk mitigation instead of risk avoidance. (policy/procedural)	ISSUE/BARRIER - POL (APPLICATION)/Need	379	Pol. Application/Need	Should implement procedures that provide needed risk mitigation but not risk avoidance.
	407-We understand the DoD rules and acq piece and why they are there, but we aren't competing in the DoD environment. Our competition can go out and procure whatever they need. There are some areas where best of breed/best practice for some of these programs whether your evaluating outcomes or actually looking at content to deliver we can't get to because of the restrictions.	ISSUE/BARRIER - POL (APPLICATION); TECH (NEW ACQUISITION)	26	ISSUE/BARRIER - POL (APPLICATION); TECH (NEW ACQUISITION)	Unable to employ best practices.
	368 - did was lay out amazon's cloud security posture, at the time it was IL2 not sure if they are IL4 yet, we try not to have any PII on our system. It was not going to be a big deal for us to move. We are completing unclassified up to	ISSUE/BARRIER - POL(PII)	025, 348	Pol. Incompatibilities	(PII compliance that assess vulnerabilities and threats and allows for a much broader access to users.)

	FOUO. (policy/procedural)				
c. What internal cybersecurity protocols most effect these challenges?	026- The people that generally run these systems are IT professionals and raised on the IT side of the house. Our experience is educational tech is different and yet rarely do we have educational technologists involved in the identification and procurement of these systems. (policy/procedural) (resource availability)	ISSUE/BARRIER - POL (APPLICATION); TECH (NEW ACQUISITION)	362	Pol. Application, Tech. New Acq. and Update	Challenges remain in understanding the importance and difference between information technology and educational technology.
	405-A product we were able to procure under the $$ threshold probably mapped to the product we would have liked to have ended up with, but it took twice the amount of paperwork to get through to the next threshold, so we were stuck making a suboptimal choice between budget and paperwork.	Pro. Internal Process/RES	362	Pro. Internal Process/RES	Lowest price technically acceptable vs. best value argument.
3. Describe to me your organization's top three cybersecurity barriers/challenges impacting DL Modernization.	022 - Our #1 barrier is getting SW, learning tools on the other military networks. JAVA updates completed by end-users. SW/LMS on common ground (policy/procedural)	ISSUE/BARRIER - PRO (TIMING)	362, 026	Pro Timing	Interoperability.

	379 - Cyber security policy implementation is the #1 influence on schedule and cost of fielding capabilities. If you execute the RMF as a DoD CIO intended, we could be much faster than we are right now. I have a self-appointed inquiry that I've written of 70 findings of fact a dozen opinions and recommendations on how we can change this within the XXX. We really need top level policy reform for cyber in the XXX. If they knew how much this influenced cost/schedule they would take it more seriously. (policy/procedural)	ISSUE/BARRIER - POL (UPDATE/APPLICATION/INCOMPATIBILITIES)/Need	026,346	Pol. Update/Need	Resource needed, cost and impact models for capabilities with considerations for cybersecurity.
	368 - Access, the XXX seems to take a very strict interpretation of all the DISA directives to the point of we have issues even in our enterprise network accessing content that's necessary. I'm not sure if	ISSUE/BARRIER - TECH (UPDATE/INFORMATION); ISSUE/BARRIER - POL (APPLICATION)	026	Tech Update/information	Policy application/interpretation. Accessibility/interoperability.
	026 - The assumption that education technology is a subset of IT is part of the problem and challenge. when we talk about DL and reaching out to our student, a majority of our students do not consume or engage educational content on govt systems. This is the biggest challenge, those who provide those capabilities/materials are saddled with reqs to use systems in fact most of our students will not be using/expecting when them come to consume those products and	ISSUE/BARRIER - POL (APPLICATION)/Need	368, 026	Pol. Application/Need	Sourcing sw/hw and finding solutions to meet the needs when saddled with policy requirements to use the system outside of the DoD domain. (outsource)

	services that we are charged with producing. (policy/procedural)				
	380 - from a technical standpoint we have to dedicate the right ppl that can implement those types of changes, it comes down to money/resources to pay for the expertise and the actual time for those ppl. That's time that they would be taking away to support. (resource availability)	ISSUE/BARRIER - TECH (UPDATE /INFORMATION) (INSTRUCTION/DEMONSTRATION)		Pro. Internal Process	Responsibilities should be aligned with the resources available, but duties should lie within areas of specialty or appropriate skill levels to manage compliance/policy changes.
	382 - The timeline to get the accreditation processes through the hurdles that have to be met to get it signed off in a timeframe that is relevant for the warfighter that's on the front line who's trying to get an app in front of them, and the different orgs groups that want to argue about who has the approval process. (scheduling)	ISSUE/BARRIER - PRO (TIMING) ISSUE/BARRIER - POL (INCOMPATIBILITIES)	026	Pro Timing/Internal process	The accreditation process could be further streamlined by sharing lessons learned.
	381 - I think the pace of technological innovation is changing so rapidly by the private sector. The DoD is having to keep up with a lot of the advancements that are taking place. (policy/procedural)	ISSUE/BARRIER - PRO (TIMING)	026	Tech New Aqu.	Fungible references.

	379 - They have to be sitting at a desktop to be able to do the training. XXX is transitioning, we aren't using static lines we are using a virtual desktop environment, so you're not locked into a classroom. Since your using virtual servers you can do different content because it's not hard loaded on there. It makes IT somewhat easier (technical)	ISSUE/BARRIER - TECH (UPDATE /INFORMATION)	025	Tech Update/information	Cost effective solution. (Risk mitigation vs risk avoidance)
a. Describe possible causes/root causes and their sources.	368 - We found that sw encryption does not lend itself to delivery of interactive multi-media. It causes a lot of timeouts/lags. (policy/procedural)	ISSUE/BARRIER - POL (APPLICATION)		Pro Timing	Utilized enterprise content management solution to address continuous cybersecurity compliance.
	026 - a fundamental tension where there are capabilities/appetites/reqs that fall well outside the rulebook of IT solutions inside the walled gardens yet those are the standards that the content developers are held to when it comes to creating those products, sourcing sw/hw and finding solutions to meet the needs. They have to operate inside the DoD domain but deliver and be consumed and engaged with students/materials outside of DoD domain. That fundamental tension creates a lot of difficulties we have when it comes to how we execute our mission from the service provider side as opposed to the consumer (student side). (policy/procedural)	ISSUE/BARRIER - POL (APPLICATION); PRO (EXTERNAL PROCESS)/Need	022	Pol. Incompatibilities, Procedures Internal/Need	Sourcing sw/hw and finding solutions to meet the needs when saddled with policy requirements to use the system outside of the DoD domain.

	381 - If there was one problem I would look at the risk management framework as a first step. you need to know what you have and know what's connecting in your network, so you know how to secure it, appropriate mitigation, counter measures. (technical)	ISSUE/BARRIER - TECH (INSTRUCTION/DEMONSTRATION/Need		Tech. Update/Need	Identified need; integrated project team implications, (instruction/demonstration) .
	362 - A product we were able to procure under that threshold probably mapped the product we would have liked to have ended up with taking twice as much paperwork to get through the next threshold, so we are stuck making a suboptimal choice between budget and paperwork. We needed to be under 1M, when you went over the paperwork, timeline doubled and so it wasn't something we could do with an accreditation finding looming that needed to be fixed and so under a Million for student information system for an org our size left us with choosing from the bottom 1/3 of the industry. (resource availability)	ISSUE/BARRIER - PRO	026	Pro. Internal Process	Lowest price technically acceptable vs. best value argument.

b. Are the causes for the described cybersecurity barrier common to other DoD services and organizations?	026 - This point is the #1 tension that exists in this business. It's the tension between the desire to maximize information security from those that control the security side and maximize student accessibility from the education side. We want student to have access to this anywhere/anytime and to make their accessibility easy and the network security side complicates that effort and the ultimate success in security is no one has access to anything. It's also the industry best practices that we can't employ because of the restrictions placed on us. (policy/procedural)	ISSUE/BARRIER - POL (UPDATE/APPLICATION/INCOMPATIBILITIES)	379, 368	Pol. Update	Disconnect between cyber security and accessibility.
c. What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0-no impact, 1-minor impact, 2-moderate impact, or 3-major impact?]	022 - Software and LMS on common ground. Major Impact. We lose classes because of it. (policy/procedural)	ISSUE/BARRIER - POL (INCOMPATIBILITIES)			External processes for cybersecurity compliance impede collaboration.
4. What are three work arounds/best practices that you have identified to mitigate those cyber security challenges?	380 - Higher level, First it's our ppl/training. In order to touch the network here administratively you have to have security plus training. OS training relative to whatever system you are working on and vetted by whatever engineering outfit... (resource availability)	ISSUE/BARRIER - RES (HUMAN CAPITAL)	26		Stringent policies and security sw tools are not enough to secure the network. Best practice is to have someone that understands the compliance and system at a high level.

	373 - Anything we design and subsequently develop, in the design phase we have to take into consideration the cyber security constraints at the very front. If you don't understand how the network works you basically run a big risk of deploying something later on that has to be significantly modified because you didn't take the constraints or the operating environments into consideration. Combo network awareness, ppl, sw itself. (technical)	TECH (NEW ACQUISITION)	381	Pro. Internal Process	Modifying, adding and deleting requirements after a project is under way greatly increases cost.
	379 - In some cases I have fielded something with and given personal assurance that you should be able to use this in a disconnected stand-alone config as it was intended without the addition layers of control. You can either conduct training or I can dot the I's and cross the T's. I locally accept the risk in training using this system w/out the sig on the ATO doc to do it. That's few and far between. In other areas it ends up being varied time, leadership intensive, pleading your case to run it up the chain. To go through the acquisition command C4 directorate and CIO to say make an exception to policy because we can't get to what you want us to within the budget and time. They in turn will write a long letter (ATO)with do's and don'ts but we will let you do it anyway. A great deal of our stuff operates that	ISSUE/BARRIER - POL (INCOMPATIBILITIES)	025	Pro. Internal Process	POC took personal responsibility for maximum acceptable risk.

	way. We will never get the $ to implement the controls that they would want us to and it limits the freedom. (resource availability)				
	382 - Challenges we are constantly working with folks in leadership to address ways forward, products, pieces, parts, all of that comes to the table. We work through the issue to try and streamline but it's the bureaucracy is one of the biggest things. (policy/procedural)	ISSUE/BARRIER - PRO/Need	379, 025	Pro Timing/Internal process/Need	Agility needed. Fungible reference.
	362 - On the academic and education side, I'm not saying there needs to be a separate regulation but there needs to be some exception based on content that you are teaching. Everything we do we look at web first.	ISSUE/BARRIER - POL (APPLICATION)	026	Pol. Update	Recommendation of cybersecurity policy application as it applies to content.
	368 - Our security posture is a defense in-depth posture. Adobe expertise manager itself has been FedRamp accredited. The sw itself. So, we found maintain our security posture with FedRamp sw was not going to be an issue. It was bringing the sw into our current environment. (policy/procedural)	ISSUE/BARRIER - POL (APPLICATION)		Pro. Internal Process	Amazon web services-data migration. Utilized enterprise content management solution to address continuous cybersecurity compliance.

a. Are these workarounds common to other DoD Services and Organizations?	368 - we are implementing student ID #'s - The concept right now is we authenticate through DMEC, we will authenticate using the EDIPI # but we won't store this in the system, it's for the initial authentication. Once in the system it will be the student #. (policy/procedural)	ISSUE/BARRIER - POL (APPLICATION)	379	Pol. Application/Pro. Internal Process	Implementing a new authentication process
	382 - In a nutshell it's constantly keeping your eyes and ears open to what's going on in the commercial industry, web. Paying attention to all possible avenues that you have and pulling it into some kind of synopsis that you can try and get an understanding of where it might go but there isn't a way to prepare for it in today's market. (policy/procedural)	ISSUE/BARRIER - PRO (TIMING)	379	Tech Instruction/Demo.	Fungible reference.
5. Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of: a. Manning	380-from a technical standpoint we have to dedicate the right ppl that can implement those types of changes, it comes down to money/resources to pay for the expertise and the actual time for those ppl. That's time that they would be taking away to support. (resource availability)	ISSUE/BARRIER - RES (HUMAN CAPITAL)		Pro. Internal Process	Skills and training required by assigned personnel.
	381-Orgs also face shortage of skilled IT/cyber sec professionals. It's not an easy problem to solve. Maybe, what orgs need to look at is outsourcing security or focus on what their core competencies are and partner with other orgs and bring some economy to scale. We have the similar applications can	ISSUE/BARRIER - RES (HUMAN CAPITAL)		Pro. Internal Process	Cost benefit (outsourcing gives you access to specialized, fully trained, and experienced talents)

	we employ common safeguards in place and that way we can keep up with the adversary out there? There isn't enough money to go around. (resource availability)				
5. Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of: b. Training	382 - It's going to be all of them. It's the properly trained individuals that are trained to work in the environment that is constantly changing. The ability to refresh tech as it's available in the industry to keep us in the game that's going on with everyone else that can go to Lowes or download on the web to use and practice with as well as have ppl in mgmt. understand that the amt of info that has to be looked at. (resource availability)	ISSUE/BARRIER - RES	026	Pro. Internal Process	Skills and training required by assigned personnel.
	381 - From my perspective, when ppl say these are cyber obstacles, what one considers obstacles might be a capability put into place to safeguard the network. (policy/procedural)	ISSUE/BARRIER - POL (EXTERNAL)		Pol. Application	Disconnect (RMF process).
5. Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms office. Equipping	022 - we are focusing on staying in line with our strategic plan. How do we focus on design, maintain and teach the classes of the future? How do we design the classroom of the future? How do we have a STEM class? We have an electrical engineering class per policy it has to have 7 students to run but we only have 3 on campus.	ISSUE/BARRIER - PRO (INTERNAL PROCESS), ISSUE/BARRIER - RES		Pro. Internal Process	Access and authentication policy implications.

	(policy/procedural)				
	379 - Faster isn't always better, there's a reason why there are small doors on cells in prisons so you're not a risk of violent harm from a prisoner because of the small door. We can use the same theory in cyber space. Minimize the amt of damage that could happen from a successful exploitation but make it as available as possible for as many users as possible. I think when we take FOUO and PII and we make it so hard to access them we drive away the users that need access to it when we could make it more accessible to authorized users and minimize the impact of a hostile actor if they did get through to access the data. (policy/procedural)	ISSUE/BARRIER-POL (APPLICATION)	382	Pol. Application	Accessibility. Fungible reference.
	368 - Access, the MC seems to take a very strict interpretation of all the DISA directives to the point of we have issues even in our enterprise network accessing content that's necessary. I'm not sure if that will get better or worse so access to us is a big deal. We would like to come up with the ability to allow the user to BYOD type of access, so they can get access to content on their iPhone, Samsung without much	ISSUE/BARRIER - PRO (EXTERNAL PROCESS)	368(?)	Pol. Application/Pro. Internal Process	Accessibility. (IT/ET?)

	effort. (policy/procedural)				
6. Describe how DL cybersecurity policy impacts decision-making process with regards to – a. Hardware	022 - The end-user/endpoint we don't have control of that. (policy/procedural)	ISSUE/BARRIER - PRO (EXTERNAL PROCESS)		Pro. External Process	Access and authentication policy implications.
6. Describe how DL cybersecurity policy impacts decision-making process with regards to – b. Networks	022 - [Network-]We don't always have control of connectivity, video delivery, java technology etc. (policy/procedural)	ISSUE/BARRIER - POL(INTERNAL)		Pro. External Process	Disconnect between internal policies prohibit DL delivery.

6. Describe how DL cybersecurity policy impacts decision-making process with regards to – c. Cost	362 - If you go back to that vendor who was selling that DL or educational content and tell them they need to step through FedRamp now at the tune of over 1M and 100K annually to maintain it and they look at the size of the customer and there are going to walk away. When we wanted to replace our student information system according to the DoD institution rules because we were going to spend more than 500K we had to go through the defense business transformation process and that encumbered us with 450 pgs worth of approvals. We initially had to get approved the problem statement that said yes, an acquisition was the right solution to solve our problem and then we had to submit additional paperwork that demonstrated that an SIS acq specifically the one we were going after was the right one. All total it was 200k+15 mo before we could get to an award to the vendor. (policy/procedural - resource availability)	ISSUE/BARRIER - POL (INCOMPATIBILITIES)	379, 025	Pol. Incompatibilities	Acquisition process is cumbersome/bureaucratic. (timing)
7. What cybersecurity challenges does your organization expect in terms of movement to cloud services?	022 - We have Challenges with what impact level we need for the material. Most of our stuff is below FOUO. Going forward the policies that direct that is a key interest to us. Do we need to pay more for perceived secure storage? (policy/procedural - resource availability)	ISSUE/BARRIER - POL (INCOMPATIBILITIES)	362	Pol. Application/Incompatibilities	Org picked a platform that had the level of collaboration and security they required. Concerned with content classification policies when moving to a cloud environment.

	386 - We do have a questions/concerns with creation of content and how much content is going to have to be transitioned from school house content to DL content. (instructional concerns)	ISSUE/BARRIER - TECH (New ACQUISITION)		Tech New Aqu.	Coexistence of legacy and modern applications.
	373 - A decentralized approach from the military protection perspective makes sense, it's costlier. Costs drive your decision making and those are some of the risks that will happen. (program costs)	ISSUE/BARRIER - RES	368	Pol. Update	Data protection
	362 - There top level of what they can provide is half of what we need to run. When their decision to move to the Cloud by 2nd quarter of FY19, they are uncoordinated with 4th estate stakeholders. There is significant impact. (technical)	ISSUE/BARRIER - TECH			Concern with storage space/bandwidth.
	405-We don't have a problem with moving the system itself. We do have questions/concerns with creation of content and how much content is going to have to be transitioned from school house content to DL content.	ISSUE/BARRIER - TECH	26	ISSUE/BARRIER - TECH	Resources to transition.
	381 - If there was one problem I would look at the risk management framework as a first step. you need to know what you have and know what's connecting in your network, so you know how to secure it, appropriate mitigation, counter measures. (technical)	ISSUE/BARRIER - TECH (INSTRUCTION/DEMONSTRATION)/ Need		Tech. Update/Need	Identified need; integrated project team implications, (instruction/demonstration) .

	380 - Understanding what cloud really is to an IT guy that really knows what it is, is a buzz word. Locations/resources and so forth. It easier to protect and it's also a big target. (instructional concerns (program)	ISSUE/BARRIER - PRO/Need	025	Pol. Application/Need	Storing data and applications remotely can cut IT costs dramatically and speed up your operations but orgs will still need to protect the information put in the cloud.
a. How would the DoD moving to a consolidated cloud effect your organization? What considerations are (or would you be) worried about?	022-We are a DoD/DoN org so we have to abide by those policies if they envelop outside of just their networks. A lot of organizational policies concerns because we manage our own network as an edu. There is worry there that they would someday. (policy/procedural)	ISSUE/BARRIER - POL (INCOMPATIBILITIES)	025	Pol. Incompatibilities	Org picked a platform that had the level of collaboration and security they required. Concern is policies will restrict local authorities.
	379 - The XXX does system level security process worse than any of the DoD components. We unfortunately have a document/checklist approach to cyber security. It's about going through the list of things you have to do and implementing more is better security controls and it increases the cost of fielding a capability because we are focused on patching and compliance rather than fully defined risk. (policy/procedural)	ISSUE/BARRIER - PRO (INTERNAL PROCESS)		Pro. Internal Process	Current policy compliance is focused on avoidance, rather than mitigation.

	362 - When we talk about conceptually, if MILCLOUD was to offer a desktop as a service, amazon does this on their commercial cloud side, if DISA were to provide that we could simply have a remotely acceptable viable web desktop analog for our users we don't manage it, we don't have to accredit it, that's a value. (technical)	ISSUE/BARRIER - TECH			Recommendation.
	346 - In most cases moving to the cloud version of a product means you need to abandon whatever customization you might have made to the product because it's not your card? your modifying which is the case in a non-based cloud where you've got your LMS running at your local org but instead your renting a space? (some of the customization that you can do to exchange records back and forth on the card that you own you cannot do on cloud-based version) (policy/procedural)	ISSUE/BARRIER - PRO (EXTERNAL PROCESS)	346	Pro External Process	Customization in the cloud is a concern.
8. If you had a magic wand, and could wave it and solve one problem, what would that problem be?	022 - The ability to manage the workstation on the students and what we need for academic delivery. Ex. I need a specific SW on a student's laptop or work computer, if I could wave my wand and deliver content easier. (policy/procedural)	ISSUE/BARRIER - PRO (INTERNAL PROCESS)		Tech. Update	Identified need (Infrastructure as a service?).

	346 - If you could do one thing and the biggest thing that affects DL is the unpredictability what are the stakes and the enforcement of those stakes with a host-based security system (HBSS). It costs a lot to create DL, we have to have some reliability, dependability if we put capability in DL HBSS wants to turn it off. (policy/procedural)	ISSUE/BARRIER - POL (INCOMPATIBILITIES)		Pol. Incompatibleness	When designing a capability, it's important to involve security (and experts from other areas) on the front end.
	380 - Resourcing in general but if I had a magic want, no one could hack us. (resource availability)	ISSUE/BARRIER - RES/Need		ISSUE/BARRIER - RES/Need	Identified need.
	026 - Cybersecurity, treating edu tech with the exact same brush stroke as Information technology because that comes with a lot of policy, legal, legislative baggage as far as what's necessary to acquire/use/deploy and the nature of the business that we operate on there isn't the necessity to ensure a bulletproof digital frontier and be as non-permissive as the NIPR is. (policy/procedural)	ISSUE/BARRIER - POL (INCOMPATIBILITIES)	362	Pol. Update/Incompatibilities	Policy implications – information technology vs educational technology.
	368 - Better balance between security and access. (policy/procedural)	ISSUE/BARRIER - POL	026	Pol. Update	Policy implications – information technology vs educational technology.

Appendix III: Interview Data

The purpose of this research is to interview government stakeholders to identify the opportunities and challenges associated with DL modernization. The research will explore and describe existing barriers and categorize them thematically, for the further purpose of recommending solutions.
Specifically, the objective for this research will be as follows:

- Determine what type of barriers exist with respect to distance learning programs
- Categorize and rank barriers
- Identify potential causes for these barriers
- Recommend possible solutions

PIPS ADL Task 5b and 6 Research Plan Question Overview

011

Task 5(b) Semi Structured Interview

Final goal: Task 5b - Identify the opportunities and challenges associated with distributed learning (DL) integration and provide (specific actionable) potential solution approaches associated with related policies that may affect implementation of DL.

Intro Script Task 5b

The Potomac Institute for Policy Studies (an independent, 501(c)(3), not-for-profit public policy research institute in Arlington, VA) is supporting the Advanced Distributed Learning Initiative (ADL) in a task to explore distributed learning (DL) modernization best practices.

As part of our task, we are interviewing government stakeholders to identify the opportunities and challenges associated with DL modernization.

These interviews will directly inform our research on identifying potential pathways to address the challenges of DL modernization related to cybersecurity.

This research aims to identify root causes that lead to barriers in getting new systems the authority to connect/authority to operate (ATC/ATO) within cybersecurity processes.

We are interested in discussing the successes and barriers you and your organization have had with navigating the implementation of new DL systems and applications.

Non-attribution Statement: All correspondence collected during interviews, surveys, or through other forms of information generation will be safeguarded by the research team. Without the express permission of the interviewee, nothing he or she says will be attributed to that speaker directly or indirectly and/or released to anyone who was not affiliated or involved with the information exchange. The research protocol will not involve names as identifiers and attribute data to an interviewee through a coded system. All research material is for the expressed purposes of the research team and members of ADL.

There is a high demand for new technology; however, processes for cybersecurity hinder distributed learning modernization. Two ideas on this: there is a requirement for ADL modernization. How often and how fast is modernization required. What impact to cybersecurity requirements has on your ability to modernize in a timely matter?

The tendency of some ppl in the bldg. and some services is to chase every new idea. What happens is you can't afford it. At what point 2.1 much better that 2.0. When do you go from the iPhone 8 to 10? That reads like new technology comes out, so you have to chase it.

How do you balance modernization, affordability and mission accomplishment or the effectiveness of ADL? DoD struggles with this in a whole bunch of areas. That's when you get into the acquisition process doesn't allow you to modernize. You don't always know what's around the corner. The tendency sometimes when you're dealing with an outside contractor is they're trying to push into things you can't afford.

- The goal this research is to identify the opportunities and challenges associated with DL integration and provide actionable potential solution approaches associated with related policies that may affect implementation of DL.

  I stood up the XXXX. I understand the threat, I understand the need to defend and I understand the balance your ability to defend with your ability to operate.

Task 5(b) Interviews Question Overview

9. What are the current DL systems utilized by your organization and how are you modernizing these systems?
   How does that work for DL?

   Here are things that I currently use: blackboard in my role on the search community for the XXXX. Blackboard is how we do collaborative conferencing, share screens, audio/video interface and at the same time you can see a presentation. This seems to be a very effective tool. You tend not to bleed over.

   In my other work, I've used quip. Quip has a collaborative tool to be able to share information. In equip you don't get audio/video, you get to be able to see if someone has added comments to a working document in real-time.
   Sococco, audio/video conferencing
   Box, to share big files.
   Zume, allows you to conference calls, collaboration in real-time.
   There are a lot of programs out there that allow you to do this stuff, not necessarily encrypted, but the app has been approved. For example: if all your looking for is a collaboration platform most of these apps to be able to operate on the Mac and other platform has gone through some level of security. The challenge you're going to have to get through on some of that is enough security for DL collaboration to take place and whether that's sufficient. 2 issues: whether it's an acceptable means of collaboration in the professional world and in the business world and Is it acceptable level cyber security to ride on the backbone of the DoD network?

One of the things is “Can I easily adapt what is being used commercially so my most cost-effective means of modernization is able to take a commercial product/app and to be able to use it. If I was going to modernize my system I’d take a look, if the applications that I was using would allow me to be able to do this work and be able to operate on the .mil network. I think that’s what they are trying to do. When I do my work for XXXX, I use my Mac but I’m not on the DoD network, but I am working on .edu network.

10. In your own words describe your DL cybersecurity process related to upgrading and modernizing your systems.
    Would I’d like to be able to do on the process, Is an understanding of the DoD process for approving applications. What are the rules that DISA wants you to go by? Some of this may be off topic but it kind of gets you to where you are. On my last year on active we transitioned form blackberry to iPhone. What they did was add an app that allowed us to encrypt our data.

    There are a lot of apps out there that would allow you to encrypt. Engage DISA early to find out what the standards are to be able to operate or would I be better off in my distance learning to go to a .edu network that is separate? As a leader, I’d want to know if that is a way to protect the DoD network.
    You’re not going to do your dl learning on SIPRnet or on higher classification networks. What are you trying to protect on the NIPRnet? Keeping in mind that sometimes unauthorized access from the NIPR, ppl have to bridge the airgap, that’s how the other networks got contaminated. If you lose NIPR there is a lot of Personal information that you can tunnel in through. How do you protect the sensitive information by using the nonclass network? The question is how do you encrypt your networks to be able to do this?
    It will boil down to being able to encrypt your information. There are a lot of new apps out there. Right now, to access the DoD network you use your CAC card to gain access. The question is “Is that how you want to run your DL?” or do you want to go to an unclass network and use the 3-factor authentication? Log in, give password, send code. When I look at modernization one of the things I’d like to know is “Is there a way of doing it that allows me to keep Personally sensitive information secure before becoming a burden or on security requirements that need to be built into it? Is there a way I can do that?
    a. How do/what DoD and local cybersecurity policies most effect your processes? What is DoD’s approval process to allow a program to operate on a network or application to operate on a network. I don’t think anything can be done locally now. On any DoD network, you have to get big brother approval to put a program on the system.

       It used to be if you were a local person you could hang stuff on the network. What we found out was you can’t. All of a sudden you like something, you put it on a machine and the next thing you know it’s operating on the network and has 15 holes in it. The other this is to know what is the refresh on the application or operating program. If a flaw is discovered who is going to patch if for you? (patching policy, what’s your standard for deploying it)

The industry standard, if you find a hole in the system especially if you're an organization that is making money, for you to do due diligence you need patch your system within 30-90 days.

11. Comprehensively describe your top cybersecurity barrier impacting modernization.
    I don't believe there are cybersecurity barriers. What's affecting my modernization instead of describing the barriers is to make sure my modernization at birth is cybersecurity compliant. To know up front what the process is. I don't think it's a barrier, it's a necessity. One of the barriers is ppl treating it as a barrier instead of a fact of life.

    Describe possible causes/root causes and their sources

    I think If you're going to develop or adopt a system, cyber security should be a consideration at the beginning, not when you've decided to go with it. If someone comes in and sells you this new toy, and you decide to go with it and the cybersecurity ppl say now way, it would have been better before you made the decision to do it to get all the tickets. I would think with DoD being the enterprise that it is, maybe the ppl you're doing business with should be aligned with what the policy is on cybersecurity before they try to market you.

    The other thing If there are cyber security issues when its operating on the network that you will have an ability to deal with in a way that it's not proprietary and you pay a lot of money to get it fixed. Example: we used to buy proprietary SW and whenever wanted to make change and/or update we were charge a lot of money because they had us over a barrel. As you modernize be aware of the trends that are occurring with mobile devices and whether you are compatible in the future. (bandwidth issues, wifi) In the future ppl will be walking around with Ipads.

    i. Of the causes for cybersecurity barrier described, do you think they are common to other DoD Services and organizations? probably
    ii. What is the impact of your described barrier on your ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? If you do not deal with the issues of cybersecurity at the beginning of your modernization plan your always going to be delayed in the process so if you don't deal with it early, it will have a major impact in terms of time and money.

        I think before you decide to modernize make sure you understand where the operating platforms are going to be in the same time period that your modernizing. There has to be a good understanding of the technology of the SW and the technology of the HW is going. I'm not trying to focus on mobile devices per se, but you have to have alignment with HW/SW in your modernization.
    iii. What one to three actions would most help overcome this barrier. Cyber first, make sure your HW/SW modernization plans are aligned. What are the alternatives to the .mil network that would be workable in the future that would also guarantee sensitive personnel information. Sometimes in DL you

have to go classified. How do you deal with classified? If they wanted to, how would you do it? In DL are we ever going to be teaching at the classified level or are you go to limit your effort to unclassified.

12. Describe your main concerns (responsibilities) in DL modernization efforts of: Main concern is being able to balance modernization costs and effectiveness. When is what I have good enough, what is my pace, when do I modernize? What is the Moore's law of DL? Once you decide what the Moore's law of DL is, what can you afford? How do you best answer what is good enough? You don't always want to be chasing the newest fad/program.

    a. Hardware-
    b. Software
    c. Networks
    d. Cost

13. Describe how DL cybersecurity policy impacts your decision-making process with regards to:
    a. Hardware
    b. Software
    c. Networks
    d. Cost

    They have to be compatible with current DoD policy. They have to have sufficient cybersecurity in order to operate on the DoD network.
    When I say you have to have cybersecurity at birth, what level of security is sufficient. To where it is no longer user friendly. For the company that I work for we can see all the machines that are encrypted. When auditors come in this is what they check for. So, you want to have standardization for how you image this stuff into operating systems. The way we make sure everything is right, with the company issues us a machine they're standardized. Only one office in the company can put the image on the computer.

14. Describe your organizations cybersecurity compliance process as related to movement to cloud services? You will need to be able to prove the cloud is secure. The physical security and the Digital security of the cloud. The cloud is just a bunch of servers. Are they physically secure? Do you have a valid access mgmt. that allows ppl to have the right level of access to what's stored in the cloud? If you move everything to the cloud you have to do access mgmt. Not everyone will have access to the whole cloud. How do you do access mgmt. in the cloud?
    a. How important is to you that cloud services are standardized? Very important. That doesn't mean it has to be the same provider.

        It's all about access mgmt. Shared services is a great thing. Shared services are access mgmt. policy/procedures that allow you to access without compromising security of your data.

15. Do you have current SOPs (or other common procedures) for obtaining authority to operate/authority to connect (ATO/ATC)? Yes
    a. Within these procedures, are there specific issues that are causing the most difficult delays/cost incurrences? My assumption not everyone has the same protocols. Protocols should be standardized.

If you like to share our services, this is who you call, these are the systems requirements. This goes back to what ADL leadership has said, there has to have some standardization, so it allows for shared services to be appropriately shared if there is an operational need.

16. What are some areas related to the issue just discussed where you think the ADL Initiative can help your organization? instead of coming up with reasonable standards that focus on more the how to do rather than what of doing things. More about the how then the what.

17. (Optional/As needed) Based on _____ (just discussed topic), it seems that it may be worthwhile to dig further into the underlying cause(s) associated with this issue. Can you identify who in or associated with your organization we should talk to next? And are you willing to introduce us to them? (The point of the introduction is not to do the staff work for us, but mainly to let these contacts, who are likely to be lower in the chain of command and possibly reticent, know that we are working on a task that is important to their organization, not just another contractor on a fishing mission.)

OSD and ADL policy should enable me to do my job but give me the freedom to do what I think is best for my organization. They should be an enabler that does not stymie freedom of action or initiative. Every service will be unique in some way. Every service will have a different amount of money that they are willing to spend as well. The OSD policy should be a facilitator to do good, it shouldn't be draconian that prevents you from doing something. Freedom of action.

For example; when you go to different training courses, in the past, completing a DL course was a prerequisite for the bigger course. sometimes DL was a stand-alone thing. Say you're taking cyber security by DL, some of the stuff will be unclassified, but how it actually happens is going to be sensitive.

If you went to XXXX, what are they teaching you? Coding, reviewing activity logs, but what's actually being manipulated they don't show you.

We know that there are challenges that you face in modernizing and update in your ability to deliver DL. We are trying to survey everyone to see how we can make your life better. Find areas of consensus where we can help improve some of the processes

PIPS ADL Task 5b and 6 Research Plan Question Overview
022
Task 5(b) Interview Overview
What are the types of DL systems that you use most often? How are these systems being modernized? We have a major advantage here in XXXX. We are on an edu network. Made the strategic decision years ago to use the XXXXX and piggyback on their internet capabilities. We run all of our programs/SW on unclassified edu networks, free from the bounds on the XXXX internet. We also have a high research and education network here that high performance computing folks use. Not really familiar but can get you information on that if you need it. Our challenge is going from the edu to the service networks.

I wasn't here at the time. The amount of bandwidth and availability of learning systems at the time was probably what we used. There are cost benefits of being on the edu. Example: we don't pay for office 365. Adobe gives us a better deal.

I don't know if cyber barriers were a part of that decision at the time. I know what this place is like, talk about academic freedom was probably the underlying foundation for it and being able to do what they needed to do.

What challenges from the cybersecurity perspective do you run into? Top 3 affecting modernization. Talking about edu. We have spoken to other educational orgs and they said it was policy implementation.

You name the piece of HW/SW it won't be smooth. My experience with XXXX, it is locked down at such a level with the breadth of what we do. If we had to put the policy on every laptop, we have a large nonresident student pop, unlike the XXXXX, do the reading and submit the exam via email. All of ours is synchronicitous delivery. We couldn't operate on the military networks with any kind of effectiveness.

What do you think is the cause for the cybersecurity challenge your organization is facing?
How do/what DoD cybersecurity policies most effect these challenges?
What internal cybersecurity protocols most effect these challenges?

3.Describe to me your organization's top three cybersecurity barriers/challenges impacting DL modernization.

Our #1 barrier is getting SW, learning tools on military networks for clients on govt machines so that a class that has multiple branches can be in a common collaborative environment. Very difficult and even though we are connected to the edu network we still need to connect to the military network. Our product base gets narrowed down pretty quickly to the least common denominator to make that connection. JAVA came out with an update last year and we were dead in the water with blackboard collaborate for a number of weeks because not everyone is in sync with the java updates which are free to do, not everyone does it at the same pace or urgency. #1 SW/LMS on common ground.

On campus, our cyber challenges are workable. We spend a lot of time defending ourselves. We don't rely on other entities. We are standing up a 24-hour ops center to protect ourselves knowing that we can't let the edu be vulnerable.

a. Describe possible causes/root causes and their sources.
b. Are the causes for the described cybersecurity barrier common to other DoD Services and Organizations?
c. What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]?

Major impact. We lose classes because of it. Here's how we are dealing with it for that risk. We have been heavy Blackboard collaborate users for a number of years. Most of our DL was VTE, we have a presence in XXXX, up until 2 weeks ago we had a field office in XXXX and in XXXX where students would go to take the class. We stopped doing this because students would rather take these classes at home, at Starbucks etc.

We shifted to blackboard collaborate to provide better customer service, but we've experienced some challenges. Java was one example. We lose control of what the end user can use when they are at work so our business schools this year, because they know what other business schools use, is actually switching technologies to teach the XXXX class via XXXX. We cannot get XXXX on military networks, but we are not willing to invest the years effort needed to through the approval process for a permanent presence SW on each of the networks that they need.

What our business school is willing to do is mandate that these classes are taken off the networks. We want to see what the impact is. These are the decisions that we are making based on the products being so much better now that we are willing to take that jump.

Working through the policies/DADMS approval process. When we were looking at XXXX, we looked to see if it was authorized, can the XXXX load XXXX? We were told that they had approved it before to a group in XXXX for a 2-week conference.

We asked for it permanently. Can I quantify it? No but it was putting our mission in someone else's hand and we didn't want to do that, so we wanted to shift off the machines onto something we would have control over. Quantifying the resources to do it? We punted early.

80% region. Where we are losing some effectiveness, we aren't getting the students we could get because they have to do stuff at work.
We don't miss out on too many classes, but we are paying for a 3-person customer desk for DL. We are paying 100K on a contract to do backend support for SAKAI LMS. Because of these resource's put out front, we get things delivered.

When I go to the XXXX and I get on a XXXX computer and I monitor a class that's being taught on collaborate, it's a degraded platform on the military network. The student doesn't get the full experience. Less than 100%, it's probably 80%.

Those are the big hitters.

18. What are three work arounds/best practices that you have identified to mitigate those cyber security challenges?
    a. Are these workarounds common to other DoD Services and Organizations?
    b. What is the impact of the work around/best practice on your organization's ability to accomplish distributed learning modernization [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? *(For example, is it an 80% or 90% solution to your challenge.)*

19. Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of:

a. Manning
b. Training
c. Equipping –We are focusing on staying in line with our strategic plan. How do we focus on design, maintain and teach the classes of the future? How do we design the classroom of the future? How do we have a STEM class? We have an electrical engineering class per policy it has to have 7 students to run but we only have 3 on campus. How do we add 4 more from XXXX or XXXX to that class and run it? It's an equipping thing.

20. Describe how DL cybersecurity policy impacts decision-making process with regards to:
    a. Hardware –The end-user/endpoint we don't have control of that.
    b. Software
    c. Networks- We don't always have control of connectivity, video delivery, java technology etc.
    d. Cost

We have a cyber director here who has worked in the information warfare career field, typically he runs things down for us through XXXX network XXXX. There are other XXXX acronyms that I'm not familiar with. We don't do a lot of research on the XXXX capabilities because we find that it changes so making decisions on the current cyber posture may be good for a few months it doesn't do us good a year from now. Our faculty drives the show here. What do you want? Our game plan is to pilot it to see how it does on the network. We have an app streaming app called PORTO. We put our toe in the water to see what works.

21. What cybersecurity challenges does your organization expect in terms of movement to cloud services? We are heavy in it and doing it. We are way ahead of the XXXX in cloud extraction. We pretty seamlessly moved to office 365, all of our accounts are cloud based via Microsoft. We are part of internet 2 consortium and have a great deal from box.com for student storage. Different products offer different levels of collaboration within the enterprise. We need to pick the right program/system to allow the amt of collaboration we want.

    We have challenges with what impact level we need for the material. Most of our stuff is below FOUO.
    Going forward the policies that direct that is a key interest to us. Do we need to pay more for perceived secure storage? We use amazon web service as a third party. Compute mainly for our researchers. We are an edu we aren't under the same restrictions as some of our partners.

    Can you speak to the consortium?

    I don't really know what it is. It's an education thing here. We are members and go to conferences…we get discounts on Zume, box. It's a membership deal.

    - How would the DoD be moving to a consolidated cloud effect your organization? What considerations are (or would you be) you worried about?
      Most of our agreements have annual options. It's not going kill us if we have to shift. We would look forward to a more competitive environment if there was a federated option,

great. We get a lot of stuff at reduced prices than .mils so I don't know if that would happen.
We are a XXXX org so we have to abide by those policies if they envelop outside of just their networks. A lot of organizational policy concerns because we manage our own network as an edu. There is worry there that they would someday.

High impact/negative. We see what our partners are dealing with. We know the basic services outside. There are not a lot right now. We are able to tailor and accept risk for us. If you are part of a bigger network you're getting bunched in and caught up in that risk pool and maybe it's not proper for you. That would be our concern. We are standing up a 24 ops center because we know what the risk is increasing, and we need to respond to it. We'll do it at the right level. We have our hand on the knob. It would be negative, we would get dragged down and lose services that we currently offer.

a. If you had a magic wand, and could wave it and solve one problem, what would that problem be? The ability to manage the workstation, the students and what we need for academic delivery. Ex. I need a specific SW on a student's laptop or work computer, if I could wave my wand and deliver content easier.

We are flexible here to serve the faculty. The flexibility piece is super important, and we have that right now. Maintaining that is what we are about on the IT Side.

Cyber security director, XXXX retired O6. He doesn't know much about the DL piece, he is protecting the edu. I can put you in contact.

Yes, It's a problem out there. You have ppl like us putting band aids, partners at the XXXX and XXXX are having a harder time and need help.

PIPS ADL Task 5b and 6 Research Plan Question Overview

379
Task 5(b) Interview Overview
What are the types of DL systems that you use most often? How are these systems being modernized?

What challenges from the cybersecurity perspective do you run into?
What do you think is the cause for the cybersecurity challenge your organization is facing?
How do/what DoD cybersecurity policies most effect these challenges?
What internal cybersecurity protocols most effect these challenges?

Describe to me your organization's top three cybersecurity barriers/challenges impacting DL modernization?
Cyber security policy implementation is the #1 influence on schedule and cost XXXX. When ppl look at the XXXX and it will be 5 years before we see it in the DoD and they aren't wrong. The reason is because we don't allow the PM and XXXX within the XXXX to make the decision of what is acceptable risk and evaluate the trade space. It's made for us and we are in many cases you'll get up to a deployment decision and find out an external agency doesn't concur/or won't accept the risk your system imposes on the network and it's not how the system is supposed to work. From the federal level down the Office

of Mgmt. budget circular A130 defines the roles and responsibilities for managing information at the strategic resource for the entire federal govt. The DoD implements out from a very well written cyber security RMF DoD instruction 8510.01 it's below that level in the XXXX and to some extent the other services that it becomes bureaucratic and the intent is obscured by legalism and focus on process and check lists. If you execute the RMF as a DoD CIO intended, we could be much faster than we are right now. I have a self-appointed inquiry that I've written of 70 findings of fact a dozen opinions and recommendations on how we can change this within the XXXX. We really need top level policy reform for cyber in the XXXX. If they knew how much this influenced cost/schedule they would take it more seriously.
Describe possible causes/root causes and their sources.
Are the causes for the described cybersecurity barrier common to other DoD Services and Organizations?
What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]?

In terms of mission accomplishment and you have to have something done and it is a cyber security barrier what do you do as a best practice to accomplish this?

In some cases, I have fielded something with and given personal assurance that you should be able to use this in a disconnected stand-alone config as it was intended without the addition layers of control. You can either conduct training or I can dot the I's and cross the T's. I locally accept the risk in training using this system w/out the sig on the ATO doc to do it. That's few and far between.

You can get in big trouble even though it doesn't have any identifying information. I have done this since I was a XXXX. If anything goes wrong, which it won't, I understand the vulnerabilities better than someone who if removed from this. I'll be accountable for the consequences, but we are going to do training and do what needs to be done.

In other areas, it ends of being varied time, leadership intensive, pleading your case to run it up the chain. To go through the XXXX and CIO to say make an exception to policy because we can't get to what you want us to within the budget and time. They in turn will write a long letter (ATO)with do's and don'ts but we will let you do it anyway. A great deal of our stuff operates that way. We will never get the $ to implement the controls that they would want us to and it limits the freedom.

Example: in the 8510.01 instruction enclosure 5 to that is Reciprocity and it talks about one of the fundamental reasons for replacing DIACAP process with RMF was that RMF presumes reciprocity. In other words, if a system is developed and it goes through the RMF of identifying the security controls, implementing them, doing an assessment of the implemented controls, authorizing that for use, any branch of service should be able to use that. The authorizing official for one branch of service will recognize the valid authorization from another to use that system. It's a great theory and if we followed the RMF it would save us time and $.

I just went through a process that took 40 days to get a simple letter extending reciprocity to an application that the XXXX and the XXXX has been using for years but XXXX were not allowed to install the app. The deployment logistics model for hw because we didn't have the stack of paperwork/test results that our authorizing official could evaluate. The reason we didn't have them was because it was in the DISA database that the XXXX doesn't use. Several yrs. ago we decided we didn't want to use

emass that system that DISA provided and recommends that the other XXXX use. We have our own repository of cyber security authorization docs that is a tower of Babel. We can't use their packages in any automated fashion and they can't read ours. We use a cost proprietary tool that none of the other services use. Those are the internal barriers that are set up at the service level to prevent us from achieving the reciprocity that is supposed to exist. The users in the XXXX don't have a published set of instruction in the XXXX-if I find something that our XXXX brethren are using that we want to use (sw, hw) there are not a set of instructions that say step 1: Contact the ISSM of the XXXX and get their package and XXXX. Only the XXXX knows this and we're the ones to whom it should be least important. It's the users who need a quick 72-96 hours, week at most, to take something that's fully authorized and begin using it in their environment. That goes for XXXX. The RMF says there can only be a single valid authorization. If someone did their job right the other services should be able to honor that.
Are these workarounds common to other DoD Services and Organizations?
What is the impact of the work around/best practice on your organization's ability to accomplish distributed learning modernization [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? *(For example, is it an 80% or 90% solution to your challenge.)*
Usually our customers XXXX. Example: 10 yrs. ago the program office that I am PM for fielded a fairly state of the electronic classroom to the XXXX, XXXX. It was good and worked for 4-5 yrs. Then the sw/computers became obsolete and they need a tech refresh. Computers, new courseware and sw. They came to us and asked if they could give them new equipment. We couldn't give them what they wanted because it was conditional on the ATO being updated. If the cyber security site authorization for the classroom/config. changes and we have to go through the whole authorization process again, it's not worth it. I tried to convince them that we could help them through it, but they didn't have enough time to wait for that. One of those classrooms in now a plain classroom, not tech being used in it anymore, and the other was converted to expand the dining hall. This was done because it was so hard to update and get the authorizations to update the tech. It was fill out the long form not does this pose a quantified risk a probability tangible real-world impact. In many cases it's no. Going back to the OMB8130 Form circular that applies to the whole federal govt., it talks about the authorization decision is confined within a system boundary. You're not supposed to consider everything that could go wrong outside the system, you're supposed to look at the risks within the systems architecture boundary and see if those are acceptable. Then the decisions about connecting those systems on the enterprise network can be made with an understanding of the additive risk of each of the system if it connects to another. The process is so hard that ppl say never mind the technology, we'll do it the old way because I don't have the time to go through the steps you want us to go through.
In terms of DL going back the CAC card, if we had the XXXX training mgmt. system our cloud readiness snapshot of individual XXXX readiness that aggregates to give you unit readiness, we should be able to scan the duty bar code on the back CAC card and I would be able to pull up the stuff that is manually put in now-when is the last time you XXXX but I would also know when the last time was that you XXXX or XXXX for XXXX.
What is the currency of all your training and what is it that you need to take next. Everyone should have a menu tailored to them that shows to advance as a XXXX, the thing you need to train to for my professional education are these. You should get reminders on your personal owned device that says you need to enroll in this, plan backward from the completion date of this online courseware or you need to XXXX. When a XXXX in a XXXX, and that that XXXX onto a XXXX it should tell every XXXX in that XXXX needs be renewed by this date XXXX, or you XXXX.
Real world example-Last year we had an XXXX on XXXX XXXX and XXXXX XXXX. 2 were XXXX, 1 part XXXX. It was XXXX 21 XXXX from an XXXX that were XXXX. When the investigation was done of the 21 XXXX they found out that 7 never had XXXX training, of the remaining 14 none of them had a current cert, 2 of them had been to the XXXX in the past 2 yrs. and failed and XXXX because our training policy states you

only have to have XXXX in the XXXX. Only XXXX have to get the training. It's amazing that our training policy allowed for 21 XXXX to XXXX and only 7 had any XXXX, none of them to successfully passed it that were passengers. XXXX had passed and were current but we need a better means of tracking certs for every indiv. We need a better means of tracking these individuals. We should know everything from health to training. We have the means to do this.
I think we can address them by not using that EDIPI and anonymizing, so it's not matched to name, ssn, until it goes into the cloud and gets the hashed identification for the individual, have it in the cloud encrypt all the data, firewall in place. I think it's fairly easy to upload and ensure who's accessing it is on the high side, that their device and authentication gives them the right to access the data. It's supposed to be there anyway we're making it easier to upload and analyze. I don't think we have to change how we gain access to the data, the real challenge gathering it and analyzed in real time.
Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of:
Manning
Training
Equipping

Describe how DL cybersecurity policy impacts decision-making process with regards to:
Hardware
Software
Networks- Example: the massive inexcusable OPM data breach where my 86yr old father called to tell me that his info was stolen, and I should get a credit lock. I shared my opinion and said the ppl who took that are not looking to do cc fraud, this is state level espionage, at your age and credit rating it's never going to be a problem.

What could we have done to minimize the potential of that? They had hundreds of millions employee records in this repository going back decades and they had effectively a huge exfiltration method. Thinking about the need to access those personnel records, most retired and current fed workforce. How many do you need to access them at one time? 12 a few 100? How long should it take to access those? They had high bandwidth ability to copy those files took minutes to a few hours. Why would we put a choke point on those? You have an old dial up modem speed, you can upload quickly but everything that comes out of there is a very small amt of data you slow the speeds down. Another technique for brute force password hacking, you have huge distributed clusters, to do this hacking you use amazon web services or a bot net for distributed computing power, so they could put massive amts of computational power in cracking passwords, so they can try billions of them in seconds. The way you would combat them is called a slow hash, you could compute billions of passwords but if it takes, there's a certain hash called b crypt that a significantly magnitude of more time to take the password input, hash it and determine if it's authenticated. By slowing down the speed with which the authentication takes place you nullify the computing power on the other side to crack the password. It would take the authenticating computer several days during which time you would notice an attack happening. Faster isn't always better, there's a reason why there are small doors on cells in prisons so you're not a risk of violent harm from a prisoner because of the small door. We can use the same theory in cyber space. Minimize the amt of damage that could happen from a successful exploitation but make it as available as possible for as many users as possible. I think when we take FOUO and PII and we make it so hard to access them we drive away the users that need access to it when we could make it more accessible to authorized users and minimize the impact of a hostile actor if they did get through to access the data. Only able to steal what they can carry in their pocket not back the truck up and take the whole warehouse.
Cost

What cybersecurity challenges does your organization expect in terms of movement to cloud services? How does it affect what you do?
It has a great deal of impact, my opinion-not endorsed publicly. For those of us that were the right age and saw Star Wars, the one enduring lesson we could take away from that was "if you build a death star someone the rebels will find a way to blow it up." This is the XXXX maybe the whole DoD's strategy for the govt cloud. We believe that only we understand our stand our security needs and we have to have a govt built/manned cloud. The XXXX version of that is XXXX services. We have licensed an extremely capable data center in XXXX it's huge by DoD standards and expensive. We didn't build an energy efficient bldg. for this we used something that existed, long term lease.
If you go to a comm cloud (amazon, google, Microsoft), they build data centers where electricity is cheap. They put a premium on the energy efficiency of the bldg. because they know they will spend far more on electricity than they will on the hw that goes in it. The power usage efficiency of their servers/data/rack servers is important if you want to make a buck.

The DoD just pays the electric bill without wondering if there is a less expensive solution. On the one hand, we want to own our own facility because we think we do it best on the other hand it is much less expensive. There was a XXXX that we did for XXXX to support the decision that was recently executed for us to move our hosting from a data center in XXXX run by XXXX. XXXX is the last tenant of that data center when we leave they will repurpose the bldg. We are moving to amazon web services, amazon can more effectively host our apps, unlike the data center in XXXX, the resiliency and redundancy of amazon is far better than we could hope in the govt. We can only afford one XXXX data center, we can't afford it on either coast and real-time mirroring across the country. We get better performance from a commercial web service. XXXX has chartered the XXXX and the XXXX within that. One of the stated purposes is to accelerate DoD migration to the cloud within an emphasis on comm solutions. XXXX knows his military personnel budget and civilian personnel budget is much better spent on warfighting capabilities than on IT services. XXXX we would man that with XXXX etc. everyone with a full paycheck and entitlement and we put them in a non-deployment in XXXX. Amazon has server scripting automated the tasks and taken the human out of the process so it's more efficient. I believe comm cloud solutions is where we should be headed. I would rather have you in the operating forces than the data center doing things.

I don't have the experience to talk about fed ramp, I will make the observation. This is a pernicious problem within the XXXX. They do system level security process worse than any of the DoD components. We unfortunately have a document/checklist approach to cyber security. It's about going through the list of things you have to do and implementing more is better security controls and it increases the cost of fielding a capability because we are focused on patching and compliance rather than fully defined risk. If you look at the XXXX policy and procedures, the message traffic and guidance, we are entirely focused on compliance, patching vulnerabilities rather than saying there is a vulnerability, a future root cause, bad things could happen if a, b, c occur, what is the probability over the day/month/yr of the system and magnitude of the adverse impact if that happens. To explain this to non-technical ppl, their eyes glaze over when you talk about specific cyber security vulnerabilities, controls and defenses against them. If you think of all cyber security controls everything you do or implement is an insurance policy against a vulnerability. You can translate that directly into your personnel financial/ car/home insurance. You know how much your home and car are worth and you know what you are willing to pay in a premium. I drive a first gen hybrid that I bought used. It's worth less than 1500, I don't carry comprehensive on it, I don't worry about someone stealing it, it is not a target that is lucrative for car

thieves. I have a low insurance premium and if the improbable happened and the car was stolen or in a wreck I have set aside $ to replace it. We don't do that in cyber security, whether it's unclass low sensitivity low integrity impact system or whether it's TSSCI.
We end up insuring old lowest price technically acceptable vehicles as if they were a brand-new Rolls Royce or very expensive platform because we are using the taxpayer's money and not our own. We would never make the same decision on what cyber security controls to implement if we had to pay for it out of our own pocket. We have separated the risk acceptance for cyber security from the PM and acquisition milestone authority decision for the acquisition community that develop/fields those systems. We have a 3rd party at XXXX that determines singularly what is an acceptable risk and they no little and careless about how much cost or how long it takes or to field the capabilities. To jump through the hoops that are set up for us in terms of cyber for the highly unlikely and no impact vulnerabilities the sad fact is in many cases we field yesterday's tech at today's cost. We weigh things down with controls and not cost effective because we have the decision authority in the wrong part of the org.
How would the DoD be moving to a consolidated cloud effect your organization? What considerations are (or would you be) you worried about?

If you had a magic wand, and could wave it and solve one problem, what would that problem be?

PIPS ADL Task 5b Research Plan Question Overview
025
Started 10yrs ago because we didn't have a good contract vehicle to get content contracted. We started looking at vehicles that easier access. Ironically, I found out that we did have one, but it wasn't geared the way we needed it to be geared or had the right language in it. We assumed that, modified it, stole other contract vehicle language and released it out and was very successful. Within 18 mo. of a 3 yr. POP we already were on track to exceed the contractual funding levels. We got involved again started a new one, we actually went from one contract that had analysis, design development, and high-end PC simulations into 3 separate contracts strategically outsourced for 700 M funding ceiling with onramp and off-ramps for the vendor.
Both of those things are listed in the base contract.
The CIO does have the authority to accept the risk and do pilot/trial stuff. Our CIO has done that sometimes but it's a long road to get that approval.

They took the ball and move to a different course. That's an organizations structure that is willing to do that. For the XXXX that won't happen. Right now, they are trying to get the .edu in line with what's going on with the .mils

We don't do it. There is no workaround, we have one LMS, this is XXXX perspective not the XXXX there are other LMS' in the XXXX, one training network. you comply, or you don't host. We have told even DoD level hosting ppl that we will not host their content because it is not in line with our instructions.

We use ATLAS PRO which is GOTS LMS that we procured 5 yrs ago and have modified to work for XXXX need. If anyone in the XXXX takes their mandatory training courses generally they're using XXXX LMS to do that.

Yes, we don't have Wi-Fi in our classes.

They have to be sitting at a desktop to be able to do the training. XXXX is transitioning, we aren't using static lines we are using a virtual desktop environment, so you're not locked into a classroom. Since your using virtual servers you can do different content because it's not hard loaded on there. It makes IT somewhat easier

Correct. Not necessarily easier for the students but it makes IT in compliance better.
I can't speak to DoD policies but XXXX absolutely
Access-we have to use CAC no other authentication can be used. This is a big one. That inhibits any kind of wireless technology. That is a showstopper for that.

I don't think I can answer that. We just do, we comply.

If you had to categorize in the areas of:
Manning
Training
Equipping –I would say policy and equipping. Right now, to do DL it's going to be hard if you have to sit in a XXXX classroom or sitting someplace where you can do a CAC. CAC readers don't work on mobile devices very well if at all so that precludes that from happening and takes that potential avenue away to do that.
Describe how DL cybersecurity policy impacts decision-making process with regards to:
Hardware
Software
Networks
Cost- Where something could be just in time or a time aide to use on a mobile device we can't do that because we can't hang it because of cyber, PII issues. We can't hang it so that influences cost because we have to have them come to a classroom

I don't do IT acquisition, but my understanding is they want the Fed Ramp upfront or a reasonable thing that will be there quickly.
I think that they would. I can't speak with authority on that.
No, our comptroller doesn't think OTA's are a viable contract solution since we have our contract vehicles in place. Since we have an IDIQ there is no reason. I've heard other orgs that use them frequently.
How do they see service members accessing content for the next 2,4,6,10 yrs. There are ppl who say anytime anywhere and then you talk to cyber or PII ppl and they don't really understand. A lot of orgs are going to content anytime anywhere but if you can't get to it than what the use in having it? I think that goes back to risk mitigation instead of risk avoidance.

PIPS ADL Task 5b Research Plan Question Overview

(026, 401,402)

We provide non-resident officer professional education to the entire officer XXXX. We have 4 programs- XXXX
From an enrollment standpoint, we have over 25,000 enrolled in the programs, Active course engagement we run 11-12,000 student # on any given day.
We launched the online master's degree in 07, launched online seminars in 12 and we launched a XXXX in 16 and a new XXXX in 17.
Our methodologies are very different from other services, we try to maximize student flexibility, our student body XXXX are busy and are generally not given time to do professional education. We are competing with their off-duty time and other events. We try to maximize the flexibility to our students. We have a very student-centered approach to doing this. Students can be admitted into any of those programs and enrolled in courses any day of the week (365) because we have facilitated seminars that complete any one of those programs they can graduate any month of the yr. We have students literally starting our programs every day and once a month we graduate students from one of those programs. We offer every online seminar course every month. We do not predetermine what courses are available on any given month or term like a normal university than limit the student availability based on a universities timing. We offer all courses, every month, we allow the students to register for what they need, and they dynamically build the # of seminars by course to meet student demand 2 wks. before the start of the course. What allows us to do that is on the systems side- a highly integrated student mgmt. system and LMS that allows us to build those seminars and on the instructor side we have a lg instructor contract where we don't commit to any instructors any more than 2-3 wks. out from the start of the term and we only commit to them for that course. We 184 instructors on that contract and currently running 175-200 seminars a month. We will graduate out of those programs anywhere from 3500-4000 a yr.

It's radically different and inside the methodology we actually have for everything but the master's degree, the master's degree is a traditional program. 8 wk. fully facilitated terms where students are engaging with their peers and faculty members just like at a university. the other 3 programs are a combination of self-paced courseware where student can go through that courseware and whatever pace meets their needs and there are pts. In the program when they complete 1-2 of the courses they will sign up for a facilitated seminar that integrates the knowledge. We have to have a system that students can sign up for the self-paced courseware any day of the week and they have 4 mo. to complete those and then after the system verifies that they've met the reqs it opens up the registration. We then build the seminar to meet their needs.
To us it's not just about the LMS it's about the integration of the LMS and student mgmt. system. Currently are LMS at XXXX is Blackboard. The university is making a transition to Canvas. Originally, 2 ½ yrs. ago they contracted to replace the legacy student mgmt. system which are all homegrown locally coded from multiple mission because XXXX has a very diverse mission set. We're just one element of it. They contracted to buy a COTS product that would integrate a student mgmt. system and LMS and meet all the reqs of probably what was a dozen student mgmt. systems that existed. That contact did not execute well, we didn't get an integrated system. The learning mgmt. side was Canvas so they decided to split off the student mgmt. and the LMS and they are now going through an effort to integrate Canvas with our legacy student mgmt. system and they're going to go out on a new effort using the OPM USA Learning contract. This is the contract vehicle that IT reform is looking at leveraging across DoD. It's a lg vehicle that has a suite of LMS, there now contracting the student mgmt. sys through that and they're going to come in and analyze and do a business process analysis to basically start that effort over.

For the LMS portion we're only transitioning from Blackboard to Canvas. Canvas that they bought is not the internally hosted that most universities have but they bought the OS Canvas to put in a Fed Ramp

approved cloud environment and they have an integrator enhancing the capabilities of Canvas and working the integration with the student mgmt. system. From the cyber standpoint, the fact that we were driven to everything being Fed ramp constrains the options you have available to you to solve these IT/ET challenges. Everything is treated as high risk, everything has to be Fed Ramped. We are in the education business where most ppl you're talking to are in the training business. Some training clearly gets to be very operational in nature and probably needs stringent security reqs. From an education standpoint, there's very little we do that should drive any security reqs. #1 thing-this blanket approach since we view everything in operational terms and were going to apply security reqs inherently constrains the options available, lengthens the timeline to get capabilities on and costs more money.
We run the education mission. We don't own the system, we don't have the decision authority on the system. We get what the IT community gives us. We influence that, but we aren't the decision makers, we are giving you the perspective of the operator and the challenges

Yes-the traditional DoD method of acq is the user gives a set of reqs to the acquiring agency, they acquire and give it back and it all works. The problem in this business, things are moving so quickly and their so dynamic that I don't think it's wise to use a methodology that #1 you can't perfectly identify the reqs for any given system upfront and#2 that you don't have a more adaptive spiral development methodology where you have folks demonstrating capability and then determining what capability will suite that. I think the OPM contract should be able to provide the capability.
The other thing I wanted to point out from a DoD Standpoint-The ppl that generally run these systems are IT professionals and raised on the IT side of the house. Our experience is educational tech is different and yet rarely do we have educational technologists involved in the identification and procurement of these systems. I think we tend to view whatever we need for tech as information tech. and we don't have the expertise to delineate the educational tech of that side of the business. Some of the contacts that we've been driven to use were IT contracts that didn't have educational tech expertise in their contractor's suite but there good at IT. No one who new LMS or student mgmt. systems but because of policy we were forced to use to contract because it was supposed to provide all IT and the assumption is education tech is a subset of IT as opposed to something different that has different capabilities.

Task 5(b) Interview Overview
What are the types of DL systems that you use most often? How are these systems being modernized?

We have the SME and the educators who are employees of the fed govt. who provide us NIPRnet a .mil network upon which most of our operations reside. All of those developers, SMEs are literally sitting in facilities inside of govt installations. We are provided with a very secure/robust network environment .mil domain to develop a lot of those materials however because of the challenges we talked about a lot of the tools, authoring tools, delivery tool, capabilities that are students have appetites for are not authorized to operate on said govt network.
Just recently our university has provided an internet as a service, not technically a separate network, there simply a .com pipe that is delivered throughout various locations in the university. We have standalone machines that can't talk across networks that our content developers will then use to translate the course materials developed by the SME and experts into materials suitable for consumption on the LMS. The LMS is hosted on a Fed Ramp approved (military DoD Approved) area of the .com space then of course cross a number of digital frontiers and end up being consumed by our students on .edu or mostly .com connections they may have access to or some of our students consume some of the content on .mil. There lies another challenge. SMEs who have the content in their head or

on one network have to cross the digital divide for the content developers who have the tools that speak to the appetites of most of our students that do them off the .mil We have to figure out how to get those tools to work on.mil domain because a number of students operate there as well. A lot depends on where our students are, most are geographically dispersed and doing it on their own time. Our command is in the middle of standing up a .edu. domain although it has a govt flavor to it primarily when you ask what network it is a .mil with devices hanging off a .com connection.

This goes back to the overarching challenge between Information security and accessibility. When we say we want to maximize accessibility on our student side we want them to be able to access this from work, home, cell. From an accessibility standpoint, we want every option available to them. From a development perspective, we're on the NIPR in terms of email but we can't really do course development on that so we have to have stand-alone computers that use stand-alone wireless to upload to Blackboard now Canvas. It's the constant back and forth from the NIPR to commercial net that causes tension. Maybe we move it all off. I've talked to XXX about maybe we need a training and education network that doesn't have all these reqs we are not currently on an edu we are on the NIPR or commercial.

Part of the constraint is they may be deployed and the only access they have to internet is a computer at the site. There are a lot of challenges. We want to maximize accessibility and that sometimes creates tension with information security.

The underlying info is not operational in nature and shouldn't be levied the same security reqs that an operation center is levied.
The process for a new system or piece of sw whether it's on the .mil or not are subject to the same constraints. We start with an approved products/hw list, this is the master list that the XXXX and DoD maintains, that says we've had security professionals that have combed through this code, looked at the hw and meets all the reqs to hand off the NIPR. If what we would like to explore/ use/deploy is not on the list than its subject to the XXXX cert/accred program. Which means it's a formal fairly in-depth process where you make justification and the case that this is an important req we'd like to use this plug in for this program or we'd like to acquire this hw and then it is submitted to our higher ups, Info Tech Specialists or those who have responsibility for it and they look at it. We have an XXXX program that says if it isn't already approved it has to be cert/acced before you get an ATO to use it. In order to be able to obtain an ATO it has to be subject to a DoD program, RMF, this details all the security controls, physical, virtual, technological that shore up the digital boundaries of that product and then based on the type of info there may be a requirement within the RMF that says it can't be on a regular .com cloud environment, it has to be Fed Ramp approved. If we still want to press forward, the vendor/service provider has to invest the time and $$ there service or capability Fed Ramp approved. Once this is all done, determination is made you can use this sw but you've got permission to purchase it as long as you manage it in accordance to info tech asset mgmt. system that outlines how you're going to ensure that it remains secure, that you have ppl trained. It's a fairly long process more than just justifying here's what we want. You've got XXXX instruction folded under a larger IT RMF that describes the pre/post conditions from a security standpoint that this sw/hw needs to be compliant with before it connects to the network. The rub and the irony are those requirements are levied on the use of that program/hw whether it's going to connect to the network or not. That's part of the risk determination that's made. We like our NIPR to be secure/bullet proof but the same reqs/process/vetting that's involved in attaching something to the secure network are the same processes that we have to avail ourselves of in order to acquire/use/deploy any educational technologies that may not already be pre-approved on that list.

We put in a request a yr. ago to pilot Microsoft 365, that request has been in a holding pattern for over a year. We weren't asking to do anything bizarre with it other than connect/collaborate with the Microsoft ecosystem. We use office 365 for govt justification to say these e are the things that are happening at Homeland Security, Dept. of Interior. We as part of the educational mission would like to leverage it in the same way. Could we make the case that its mission critical? It paints us into an interesting corner we technically can't acquire use any sw/hw capabilities until we get the approval for it. If we make the case that something is mission critical we are admitting that we've circumvented. It's hard to make the case because it's so hard to gain the approval to start using the systems in the first place. Usually you make that case after you receive the interim authority to connect has been granted by headquarters. Then if it becomes mission critical then you can make the case. In 2 yrs. I have not been involved in that sort of discussion. I have heard of it at HQ, maybe a cpl of months if you make the case strong enough. That assumes you have it on hand and its embedded in your ops.
It would be the option of the approval authority whoever has the authority to approve your request to connect to the network. They could come back and say deny or approved or interim. It's not something we would ask for, we say here is a capability, we've identified one tool that we think is a smart match to meet this capability and request permission to purchase and use.

What challenges from the cybersecurity perspective do you run into?
What do you think is the cause for the cybersecurity challenge your organization is facing?
How do/what DoD cybersecurity policies most effect these challenges?
What internal cybersecurity protocols most effect these challenges?

Describe to me your organization's top three cybersecurity barriers/challenges impacting DL modernization.
It's not in procurement it's in the shops that run the system. Most of our DoD shops that own these systems are IT professionals it's not the contracting ppl it's the technology shops that are largely IT professionals because that's what they do in the XXXX. The majority of the XXXX is focused on IT. This education thing is a unique university thing not a wide spread capability needed across the XXXX. The assumption that education technology is a subset of IT is part of the problem and challenge.

When you talk operationally within the XXXX it's relatively easy to confine your concerns for IT and wall that garden off because those operations are executed inside the walls of an XXXX base or DoD facility specifically when we talk about DL and reaching out to our student, a majority of our students do not consume or engage educational content on govt systems. This is the biggest challenge, those who provide those capabilities/materials are saddled with reqs to use systems in fact most of our students will not be using/expecting when them come to consume those products and services that we are charged with producing. That's a fundamental tension where there are capabilities/appetites/reqs that fall well outside the rulebook of IT solutions inside the walled gardens yet those are the standards that the content developers are held to when it comes to creating those products, sourcing sw/hw and finding solutions to meet the needs. They have to operate inside the DoD domain but deliver and be consumed and engaged with students/materials outside of DoD domain. That fundamental tension creates a lot of difficulties we have when it comes to how we execute our mission from the service provider side as opposed to the consumer (student side).

This point is the #1 tension that exists in this business. It's the tension between the desire to maximize information security from those that control the security side and maximize student accessibility from

the education side. We want student to have access to this anywhere/anytime and to make their accessibility easy and the network security side complicates that effort and the ultimate success in security is no one has access to anything.

It's also the industry best practices that we can't employ because of the restrictions placed on us.

Describe possible causes/root causes and their sources.
Are the causes for the described cybersecurity barrier common to other DoD Services and Organizations?
What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]?

What are three work arounds/best practices that you have identified to mitigate those cyber security challenges?
Are these workarounds common to other DoD Services and Organizations?
What is the impact of the work around/best practice on your organization's ability to accomplish distributed learning modernization [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? *(For example, is it an 80% or 90% solution to your challenge.)*

Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of:
Manning
Training
Equipping

Describe how DL cybersecurity policy impacts decision-making process with regards to:
Hardware
Software
Networks
Cost

What cybersecurity challenges does your organization expect in terms of movement to cloud services? How would the DoD be moving to a consolidated cloud effect your organization? What considerations are (or would you be) you worried about?
Our major command, two levels above where we sit now, are leveraging a lg OPM contract to deliver what they claim to be an integrated cloud architecture that has been accredited such that if you have a new capability or system rather than have the sw accredited, if that sw or system meets baseline config reqs and you want to operate it in the cloud environment than you don't have to go through a separate accreditation process for it. On the surface, it sounds like a great idea. It sounds like it could potentially streamline the time it would take to request/field a new system. It cuts some of the front and backend of the cert/accred process. It also promises that there is a common data lake lying below it and if you drop a new system in it and it has the right interfaces it leads to the data lake and supposedly it will read and transmit exchange data between all the other systems that are sitting in the architecture. it sounds like a great idea that will provide integration possibilities, streamline acq. timeline. I think personally as a technologist are we going to end up trading one set of restrictive acq/security reqs for another? Now instead of cert/accrd now everything needs to meet the reqs of the cloud architecture including data interchange reqs. This is conceptual. We haven't seen it to say what affect it would have.

I'm going to give you the I operate on systems perspective as opposed to implement systems. We need a flexible adaptive accessible system. I don't care where its hosted as long as it has the capabilities. The assumption is cloud services overcome all of those things, but you can clamp down cloud services like you can clamp down others. We need flexibility, adaptability and accessibility in whatever system it is and if cloud systems are the way that you get that than great. Driving the solution set is not so much our interest.
Cloud by itself doesn't mean it will be better, now you've move data storage. Your data might be available, reliable but that doesn't mean things will be better.

If you had a magic wand, and could wave it and solve one problem, what would that problem be?
Cyber security.
I think treating edu tech with the exact same brush stroke as Information technology because that comes with a lot of policy, legal, legislative baggage as far as what's necessary to acquire/use/deploy and the nature of the business that we operate on there isn't the necessity to ensure a bulletproof digital frontier and be as non-permissive as the NIPR is. If there was a way to treat educational tech with a different lens, different acq mindset so that it was easier to explore/develop/test/keep up with changes in educational technologies that wasn't saddled by a system that is by necessity and definition restrictive, that would be great.
Strategic level cyber security we would like to see a nuance approach opposed to a blanket approach. The nuance being driven by the kind of data your trying to secure.
PIPS ADL Task 5b Research Plan Question Overview
362 (XXX)

The reality is we haven't acquired much for a number of years, SAKAI has been our LMS for over 10yrs. We engaged a company within the SAKAI community that does customization for us so outside of that our work in the imperial community the only quasi learning tech tool that we've acquired was for lecture capture which we did last yr. I'm not sure that we are a wealth of experience for you because we haven't done much. We are working on procuring an external portfolio tool that will replace what SAKAI is no longer going to support.
It may be a definition issue, XXXX point is spot on about our DL capabilities, we buy a lot of other tech tools here at the institution and you go thought the typical pains of the govt acq cycle.
We have some advantage over some DoD orgs from an IT standpoint we operate 2 networks (.mil and .edu) We make some exceptions on our .edu commercial network. We have some capabilities along the DL lines that comes through acq over the yrs that I don't think we would have been able to do if we were 100% NIPR org. Those difficulties still exist but we somewhat side step them based on our being on edu, self-contained when someone asks if we are protecting the DoD gig we can say we don't touch the DoD NIPR. An example on the DL side as far as acquisitions and challenges. If you look at one of the RMF rules controls cyber security and the cloud SRG policies that are out there is while the language is in there that say's there going to make a risk assessment based on the type of data they have on a level that needs protection in practice when you're going through acq it does not necessary play out. What I mean by that is a cloud provider that does not have a Fed Ramp, does not have their cert that they need. What ends up happening is the answer is no. you can't get to it. We are 1 of 1 XXXX within the DoD. I'm not competing against DoD and the info I need to store in those systems is public. The blood clotting cascade you can find in any textbook, I don't need to protect the data in the same way, yet we're still hampered by the DoD acq rules. If you go back to that vendor who was selling that DL or educational content and tell them they need to step through Fed Ramp now at the tune of over 1M and 100K annually to maintain it and they look at the size of the customer and there are going to walk away.

That has been a challenge, some of that you see in the ADL gaps report where they talk about deficient contract language for procuring compliant learning tech, in the report their talking about a standard out there but there are 3-4 acq things in the report we would echo and support.
When we wanted to replace our student information system according to the DoD institution rules because we were going to spend more than 500K we had to go through the defense business transformation process and that encumbered us with 450 pgs worth of approvals. We initially had to get approved the problem statement that said yes, an acquisition was the right solution to solve our problem and then we had to submit additional paperwork that demonstrated that an SIS acq specifically the one we were going after was the right one. All total it was 200k+15 mo. before we could get to an award to the vendor.
A product we were able to procure under that threshold probably mapped the product we would have liked to have ended up with taking twice as much paperwork to get through the next threshold, so we are stuck making a suboptimal choice between budget and paperwork.
We needed to be under 1M, when you went over the paperwork, timeline doubled and so it wasn't something we could do with an accreditation finding looming that needed to be fixed and so under a Million for student information system for an org our size left us with choosing from the bottom 1/3 of the industry.
We understand the DoD rules and acq piece and why they are there, but we aren't competing in the DoD environment. Our competition so to speak is XXXX and when they can go out and procure, there are some areas where best of breed/best practice for some of these programs whether your evaluating outcomes or actually looking at content to deliver we can't get to because of the restrictions.
Typically, they happen at the same time. We'll have a list of 11 vendors and we narrow down based on capabilities and what the mission needs are but one of the criteria is always if it's a fast solution do they have everything that's required in the cloud SRG are they Fed Ramp, that's one of the evaluation criteria for all 11. This is weighted pretty heavily so we may have the top 3 get eliminated because they aren't certified, they don't have the Fed ramp, their best of breed but they also don't offer an on premises solution meaning you buy cloud or what they offer or you just don't use it and they end up getting thrown out or we go to our AO and say well now we will need to access the risk of these using them outside of DoD, Fed Ramp and/or acq guidelines, DFAR is that risk acceptable. On the academic and education side, I'm not saying there needs to be a separate regulation but there needs to be some exception based on content that you are teaching. The content we are delivering is OS. You may look XXXX and say you have foreign nationals you've got scenarios' that are sensitive and classified…ok. Maybe that educational platform needs to be a different level. DODIA is a 4th of state, there doing k12 education. Math and English, do I really need that protected at the classified level?
10yrs ago everything at the university was on NIPRnet. The faculty/students were complaining. Our .edu presence at that time sat in the library/student lounge areas but wasn't used outside of those locations. We looked and realized we needed to be the exact opposite. Everything we are doing is academia, students can't open a video that the instructor puts in their teaching content. A 3-min video would take 20 min because of bandwidth restrictions/buffering. We used the same justification to say we are secure we can provide a better service and manage risk better. We switched everything to edu and we have a very small .mil footprint. They are completely separate but everything we do is on .edu. other orgs are having the same problem, the XXXX in XXXX who educate all the XXXX (XXXX etc.) have asked us to provide their edu services for them. The outcome-we went to a 3rd party vendor and had them access it and came back to say we think it would make sense for XXXX to provide edu and academic services to XXXX to solve these problems.
Some examples that I will tell you we've had. Doing medical research, we have research projects that have been endorsed in tropical medicine. This was a collaborative effort with the Chinese. There is no way your collaborating on .mil that collaboration came to a halt based on network restrictions.

We have faculty members who are trying to get out to professional organizations that are specifically tied to their job functions here and we'll find that the IP address that the org is on is part of a class C that is blocked by DoD. The IP itself isn't bad but the class C group of IPs because there is a bad actor in that group. Trying to get the IP unblocked could take weeks/months.
Those types of issues we've run into repeatedly. We've got XXXX exams that have to take place. A lot of times the National exam providers have very specific ideas on what they will allow at the desktop. Being on edu allows us to control that.
The one additional and ongoing is trying to collaborate with the XXXX for high profile XXXX research, 9 figure funded program. It's working right now because we are on edu to move back to NIPR. It restricts our ability to access these public websites and we've been working with DISA for 9 months trying to get them to unblock 2 unsafe websites. It's not a priority. When you think about the larger DISA/DoD mission, that makes sense but in terms of furthering the research/education there is a significant disconnect there. There needs to be a type coupling between the authorizing official and the mission owner. Some of the conversations taking place are concerning they seem to have forgotten that we are not an IT org first, but we are supporting warfighters with IT or educational tech depending on your preview. We are a XXXX, we are a system that is meant to facilitate and extend abilities and when we disconnect the mission owner from the authorization process that we will always fail.
Another example: Collaboration suites. We've been on one for 9 yrs. It has saved us a significant amt of $ and if we took what we currently have and moved it to the DoD environment we'd pay dbl. I would have 13% of the capacity I have right now and none of the collaboration tools and that was a tool we needed for academic mission and that's why we've been on it for 9 yrs. on edu. Within the 4th of state they are entertaining moving to that now. Implementation even when they get down that path will be 2-3 yrs. down the road. That's 10-15 yrs. too late when you talk about academic environment and being able to compete with programs that are attracting students around the US and they've had it longer than we have. It does come back to acquisitions we went through a number of gyrations trying to get that on a contract We actually had help from PEO EIS because they were doing a pilot and we piggybacked. We originally had our own contract, went to PEO EIS and then back to our own. Those are the some of the challenges. Academic cannot be 10-15 yrs. behind in academic tech acq.
There is specific contract language for any IT systems, generic boiler plate, that is put in. We have added some additional tools on top of that collaboration suite for example to meet DoD reqs that would not have traditionally been there.
The collaboration suite off the shelf has a lot of capabilities for mobilized mgmt. tracking mobile apps and managing the data stored in drive but we found when we looked at that against DoD reqs are it may be 75% of them and the big ones but the remaining 25% we needed to buy a tool to lay on top of it. We bought a mobile device mgmt. tool and supplemented what came off the shelf for the collaboration suite. We bought a cloud security firewall and document monitoring tool that sat on top of drive and monitored ssn etc.
It's a new fish bowl every time around. Our team will contact DISAs battle captain at FT Meade to say here is our issue what do we need to do in order to resolve? They end up sending a different form from before, we fill it out, it either gets lost or we'll need to resubmit with modifications or get someone's approval. We'll be required to cite regulatory authority and for the particular case of getting the website unblocked is a website that support secure digital certificate and that website is supposed to be trusted based on DISA provided systems that we are supposed to build our mobile computers off of. They give us a template of what it should look like, we build from that. Unfortunately, there is a disconnect between their right and left hand. When we cite these things, ppl get confused, paperwork gets lost and we have to start all over again we reinitiate a few weeks later. This has been going on for 9 mo.
xApi

OS-The university moved to an OS LMS 10 yrs ago based on license cost, capabilities, hosting. We found great success. We are working with the OS comm SAKAI and extending and trying to tune the capability the best that we can. In parallel we've been working with Open LRS (learning record store) that was meant to be the first hyper scale capable and OS projects implementing xApi specs. That project is called Open LRW (Learning records warehouse) that encompasses the cattleberg? format. We are not using this today, it was one of the gaps that we found in the overall specs capabilities of either the recording and discoverability aspect of this. With xApi it's easy to create learner records. Billy did this and jimmy did that but deciding the instructor and identifying which instructor should be able to see what information they should see and how they view. It is unaddressed and unmapped territory. We are re-engaging in the hope we will be able to build something usable for ours and other communities based on strong advocate of the govt is going to pay for something and it will be OS but we do not have that in deployment today. We actually had running prototypes of this about 3 yrs ago, given other priorities, I don't need to procure something that's xApi compliant I go out to the Imperial community and work with them to say this is something that needs to be brought in to SAKAI and if necessary we fund independently a vendor to do that work. I'm probably going to Ft Bragg to see where ADL is. There are additional things that need to be done to the spec in order for us to use it.
It's really about identifying what in the SAKAI ____ is context. What context did Billy or jimmy answer a question with a particular answer ID and how do we identify the context and who is meant to consume info from them. Should this faculty member be able to see all of the info regardless of its context? It is a mapping problem which gets complicated quickly. I'm not sure an xApi profile would directly facilitate that or solve the problem. In particular because we have to be sensitive as an accredited higher education to the requirements for TALBER? sources of info as well.
100% responsive web based. We should have told you about our programs. There's a XXXX here, those students are really only here for 18 mo. the remainder of the time they are at XXXXl facilities around the world. The reach back ability is essential. Graduate XXXX program, PhD's they have some of those reach back requirements as well. There's a XXXX based out of XXXX, their programs are also all around the US at various XXXX. We've also got a graduated education office. College of XXXX that are really working with XXXX those students go through a list of programs, they'd walk out the door and have nothing to show for it. Now they are mapping them to get credits and a transcript and if they transfer in gen ed they can get their assoc. or bachelor's degree. We also have researchers that are also around the world at various times. Everything we do we look at web first. Work is a thing you do not a place you go.
Our curriculum is 90% blended.
Task 5(b) Interview Overview
What are the types of DL systems that you use most often? How are these systems being modernized?

What challenges from the cybersecurity perspective do you run into?
What do you think is the cause for the cybersecurity challenge your organization is facing?
How do/what DoD cybersecurity policies most effect these challenges?
What internal cybersecurity protocols most effect these challenges?

Describe to me your organization's top three cybersecurity barriers/challenges impacting DL modernization.
Describe possible causes/root causes and their sources.
Are the causes for the described cybersecurity barrier common to other DoD Services and Organizations?
What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]?

What are three work arounds/best practices that you have identified to mitigate those cyber security challenges?
Are these workarounds common to other DoD Services and Organizations?
What is the impact of the work around/best practice on your organization's ability to accomplish distributed learning modernization [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? *(For example, is it an 80% or 90% solution to your challenge.)*

Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of:
Manning
Training
Equipping

Describe how DL cybersecurity policy impacts decision-making process with regards to:
Hardware
Software
Networks
Cost

What cybersecurity challenges does your organization expect in terms of movement to cloud services? How would the DoD moving to a consolidated cloud effect your organization? What considerations are (or would you be) you worried about?
Negatively. We haven't talked about from an acq standpoint is academic pricing. Being forced into this mold just isn't a functionality question, it's a question of I'm going to actually pay increased cost. We had some folks out here looking at what we could get at
academic pricing whether it's hw/sw. They also looked at our network services and pretty much said. "We can't touch the prices." A lot of the academic prices if you have an accredited academic program you can get access to things that the DoD can't come close to because you are being given them almost at cost.

From a cloud standpoint one of the things we need to look is where we are at with cost, from a cyber security standpoint can you restate?

On the research side for example, we were given a mandate from 4th of state on when we needed to move to MILCLOUD. They specified this is what we can provide: up to 192 gigs of ram unto 16 cores, we have 1/3 largest sequence/processing operations in the world. The min is 1 terabyte of ram in order to load the frameworks. There top level of what they can provide is half of what we need to run. When their decision to move to the Cloud by 2nd quarter of FY19, they are uncoordinated with 4th estate stakeholders. There is significant impact.

This isn't to say the org is against this. XXXX is talking about when they came on site to talk about things. It was a very productive conversation. We talked in the beginning about our small NIPR presence and we do very little on it other than provide an opp for our military service members to get on NIPR only server. Beyond that we don't have a use for the system. When we talk about conceptually with them if MILCLOUD to offer a desktop as a service, amazon does this on their commercial cloud side, if DISA were to provide that we could Simply have remotely acceptable viable web desktop analog for our users we don't manage it, we don't have to accredit it, that's a value. In terms of academic accreditation

and sanity of business. Most of these services in terms of their implementation plan need to be opt in keep the tie with mission and technical implementation.

A lot of these mandates/ideas while they have good intentions and they are good ideas are not mapped back to real business because we haven't done a proper job of vetting requirements prior to implementation.
DL acquisition side the majority of the users in the 4th estate are training focused not education. Our bottom line has been anywhere these consolidation efforts can save money and make sense we are all in. There are 3 exceptions:
Cannot negatively affect our accreditation
Cannot deprecate existing capabilities/mission effectiveness
Cannot increase cost

If you had a magic wand, and could wave it and solve one problem, what would that problem be?

PIPS ADL Task 5b Research Plan Question Overview
7.24.18 (346,403,404)

Task 5(b) Interview Overview
What are the types of DL systems that you use most often? How are these systems being modernized? I've prepared a word document for this that I don't access to but will send. The delivery systems that we use are dictated by the interactive multi-media types that we utilize. We figure out the IMI type we need and that drives what specs we use for it. Once I get clearance to send it to you I will send you a copy of your questions about a pg. or more of explanatory material (white paper) that will answer most of your questions. The short pic is computer managed instruction (audio-scoring DL) there's? no classroom, no instructor, cost wise is most of the DL we do and that is delivered by LMS called the XXXX the 2nd IMI type we have is called, Computer aided instruction (blended solution) where there 1 instructor in a classroom, Learners which is a distance classroom there may be 1 or more of those and basically the instructor determines when the learner has completed the knowledge and CMI. Those account for most of our DL and CAI? Course Mgmt. Our course mgmt. system is largely blackboard based. The 3rd major IMI category is a combo of mobile learning and electronic publications. They are typically delivered by systems that don't score, lots of reasons why, some of that is explained in the white paper. We use 2 LMS, ALMS, Course Mgmt. systems (2) one for FOUO and one for not FOUO and our primary distribution system for mobile is called XXXX. As far as modernization, there are 2 modernization paths proposed, I put it in writing because it is easy to confuse: most of the components that are used for DL on the systems side are in an artificial construct that we call the XXXX. The intended modernization path for all of them, the LMS, XXXX training HD is through an XXXX called XXXX (XXXX) and has 5 parts the XXXX, XXXX, those 2 parts comprise what we called the XXXX DL ecosystem. The intended path was by FY23 XXXX would go FOC (full operational capability) replacing all of the stuff that supports our making IMI. That's the plan however on the horizon there's the OPM effort, OSD reform effort that has a lot of COAs. If that comes to pass we should know on Thursday. Much of what I just described DL ecosystem and some additional components that belong to XXXX may belong to OPM and one the modernization path will be dictated by OPM.
Our primary system LMS for CMI is web based, not designed in the cloud environment it's running in the cloud, it has a lot of moving pieces. The modernization path for that LMS will occur either in the XXXX

program or with OPM. To be frank the existing system will probably not survive either one, it will be replaced. As long as it meets our reds, specs, and standards we don't care
I did see XXXX on the invitation list, he would be the one to address the system side as the authoritative. The stuff I provide is informative, for authoritative, anything to do with the systems, it needs to come from XXXX XXXX (XXXX), XXXX. The other mtg I have to go this morning and the one I was already in had to do was about ppl at your level getting information from the wrong ppl and running with it. So, I can't caution enough that authoritative systems data must come from XXXX, XXXX ADL will not provide you with authoritative cyber?

What challenges from the cybersecurity perspective do you run into? I think the context of the question has to do with ADL and the cyber security issues but I think we would defer XXXX section to answer. The only thing I didn't answer is the magic wand question.
What do you think is the cause for the cybersecurity challenge your organization is facing?
How do/what DoD cybersecurity policies most effect these challenges?
What internal cybersecurity protocols most effect these challenges?

Describe to me your organization's top three cybersecurity barriers/challenges impacting DL modernization.
Describe possible causes/root causes and their sources.
Are the causes for the described cybersecurity barrier common to other DoD Services and Organizations?
What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]?

What are three work arounds/best practices that you have identified to mitigate those cyber security challenges?
Are these workarounds common to other DoD Services and Organizations?
What is the impact of the work around/best practice on your organization's ability to accomplish distributed learning modernization [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? *(For example, is it an 80% or 90% solution to your challenge.)*

Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of:
Manning
Training
Equipping

Describe how DL cybersecurity policy impacts decision-making process with regards to:
The difficulty is while moving something to .edu it doesn't fix the problem because if your transit any part of the NIPRnet, systems like HBSS latch on to whatever's running across. 90% or more of all DL is taken on a govt computer in a govt workplace which is inside the NIPRnet. While those sound like great ideas the only work if you tell them to take their DL home. Where's the content hosted, on the NIPR. This has to be fixed on the NIPRnet.
Hardware
Software
Networks
Cost

What cybersecurity challenges does your organization expect in terms of movement to cloud services? How would the DoD moving to a consolidated cloud effect your organization? What considerations are (or would you be) you worried about?
This is a question for XXXX. My information thought is -In most cases moving to the cloud version of a product means you need to abandon whatever customization you might have made to the product because it's not your card? your modifying which is the case in a non-based cloud where you've got your LMS running at your local org but instead your renting a space? One of XXXX, we can in theory make any changes to our LMS to suit our purposes. The cloud-based version is literally a rented space on blackboard.com, some of the customization that you can do to exchange records back and forth on the card that you own you cannot do on cloud-based version, if the cloud base version is unmodified box? Contracting perspective for DL content, there is a desire in the DL comm to use cloud services. They want to escape the confines of the LMS. They want flexibility and instructional design ability of movement through the content and only report back what is necessary to report. Amazon web services is the preferred.

If you had a magic wand, and could wave it and solve one problem, what would that
problem be? If you could do one thing and the biggest thing that affects DL is the unpredictability what are the stakes and the enforcement of those stakes with a host-based security system (HBSS). It costs a lot to create DL, we have to have some reliability, dependability if we put capability in DL HBSS wants to turn it off. They look at behaviors, what you can do what you can't do, and the unpredictability is hurting our efforts to modernize.

From my perspective the contracts, I understand where that's coming from we are challenged with modernizing DL content and the effort to modernize that's often conflict with the understandable needs for cyber security.

We provide a contract vehicle with our requiring activity that we use when developing training and education and very often that innovation is in conflict with the STIG? The authoring tool captivate there are many capabilities within the authoring tool that are turned off based on the STIG. Where content is published out as the authoring tool we find that many of the capabilities will not play.

Generally, with captivate we work with computer scientists(?) here in coordination with STIGS and then work with developers to get the content in line with the STIG req. We don't do anything outside of cyber guidance but very often we are blindsided. There may be a push to put a new STIG in and we are always the last to know. There is no process by which the training and education comm is notified so that we can in a timely manner correct any content coming in or being developed.

PIPS ADL Task 5b Research Plan Question Overview
(368, 405)

I'm the technical director for XXXX. I retired from active duty 10 yrs. ago and I've been in this position for 15 yrs. We are responsible for running XXXX which is the XXXX DL LMS, it is a system of systems but as far as cyber security my experience has always been requesting ATO/ATC. I've also supported so of our professional military education programs focused on Moodle/blackboard.

Task 5(b) Interview Overview
What are the types of DL systems that you use most often? How are these systems being modernized?
The current XXXX system has 3 main components, SCORM engine for content delivery, Microsoft sequel

the backside database and question mark reception for assessments and surveys. There are backside things like Lenox to mix in security posture. We also support online professional military education programs we previously had Blackboard, but Blackboard took their time getting FedRamp accredited so our contracting officer did not allow us to renew our contract. We went with Moodle through OPM's USA Learn program. Our modernization program is underway now, we are pilot 1 what that means is we procured Adobe Experience Manager which is going to be a front facing tool provides that provides individualized learning, communities of interest, communication within the tool rustice's scorm engine works inside there and we are working on integrating that with Moodle so that we are working towards creating a e-learning ecosystem for the XXXX. We will be supporting e learning as well as DL. You can take the class in the classroom or on your own however the sponsor wants to deliver the content.

What challenges from the cybersecurity perspective do you run into? XXXX is on Version 5.2 as far as the security posture and challenges the biggest thing we are facing is being one of the first lg orgs to leave a DoD enclave and move to amazon web services. The challenge there is getting ppl to understand that amazon web services is a secure environment. Because we are the first to do this on a lg scale, the challenge has been making sure controls are in place to maintain security posture.

We did, a cpl of ways, have you heard of XXXX. The XXXX has built a lg facility in XXXX and they wanted everyone, in accordance with consolidating data centers, to move to XXXX. A few of us went out and determined that they could not support us, we are several yrs. ahead of them regarding delivering content. We did some analysis and determined it would be cheaper and easier to go to amazon.

What do you think is the cause for the cybersecurity challenge your organization is facing?
How do/what DoD cybersecurity policies most effect these challenges? No, what we did was lay out amazon's cloud security posture, at the time it was IL2 not sure if they are IL4 yet, we try not to have any PII on our system. I was not going to be a big deal for us to move. We are completing unclassified up to FOUO.

We had ssn in the system but we also bypassed the EDIPI number because of rumblings that EDIPI was going to be PII, we are implementing student ID #'s, that's how we are going to get around that.

The concept right now is we authenticate through XXXX, we will authenticate using the EDIPI # but we won't store this in the system, it's for the initial authentication. Once in the system it will be the student #.

What internal cybersecurity protocols most effect these challenges?

Describe to me your organization's top three cybersecurity barriers/challenges impacting DL modernization. The XXXX was directed to do a data center consolidation so that's why we are moving. Right now, our servers are in XXXX. We are complying with the direction to consolidate. The reason we aren't going into XXXX is because we have a video service kind of like YouTube but more controlled and we allow orgs/units to upload user generated content and control it, so XXXX did not have the capability to stream those assets and then another thing we found through trial and error was the XXXX concept was a sw encryption. We found that sw encryption does not lend itself to delivery of interactive multi-media. It causes a lot of timeouts/lags. We went to hw encryption methodology and they were not able to support that so that was the biggest thing was hw encryption that kept us out.

Describe possible causes/root causes and their sources.
Are the causes for the described cybersecurity barrier common to other DoD Services and Organizations?
What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]?
Are security posture is defense in-depth. Adobe experience manager has been FedRamped. Bringing the sw into the current environment.

What are three work arounds/best practices that you have identified to mitigate those cyber security challenges? Our security posture is a defense in-depth posture. Adobe expertise manager itself has been FedRamp accredited. The sw itself. So, we found maintain our security posture with FedRamp sw was not going to be an issue. It was bringing the sw into our current environment.
Are these workarounds common to other DoD Services and Organizations?
What is the impact of the work around/best practice on your organization's ability to accomplish distributed learning modernization [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? *(For example, is it an 80% or 90% solution to your challenge.)*

Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of:
Access, the XXXX seems to take a very strict interpretation of all the DISA directives to the point of we have issues even in our enterprise network accessing content that's necessary. I'm not sure if that will get better or worse so access to us is a big deal. We would like to come up with the ability to allow the user to BYOD type of access so they can get access to content on their iPhone, Samsung without much effort.
Manning
Training
Equipping

A long time ago we used to ship out CDs of the content and found that not to be a very good method so what we'll right now is have our network folks look at work arounds to allow access to the content.

We kept it on the down low. We are authorized by our ATO to still use user enabled password. Part of the systems support is for certain spouse's that do things within the XXXX, volunteer network, so I can get to a certain amt of things on my mobile device. It's just user name/password.

Describe how DL cybersecurity policy impacts decision-making process with regards to:
Hardware
Software
Networks
Cost

What cybersecurity challenges does your organization expect in terms of movement to cloud services?
This is running concurrent with what we've was briefed last week for the consolidation. The way I understand it, the services will be moving to, I don't think it's necessarily 1 cloud, OPM as far as a PM office for licenses and integration (things like that). The way I understand it, The AF since they are

already working with OPM will streamline things and figure out how things should be done, and we will follow close on the heels of the XXXX because what the XXXX is doing and what we are doing are very similar. We don't have a problem with moving the system itself. We do have a questions/concerns with creation of content and how much content is going to have to be transitioned from school house content to DL content.

How would the DoD moving to a consolidated cloud effect your organization? What considerations are (or would you be) you worried about?

If you had a magic wand, and could wave it and solve one problem, what would that
problem be? Better balance between security and access.
PIPS ADL Task 5b Research Plan Question Overview

(332)

I've been doing this for 15-20 yrs. I started in XXXX. We were taking correspondence courses and putting them online. I've worked with the XXXX for many years doing conversion training something like XXXX before SCORM came out. 10 yrs. ago I transferred XXXX, XXXX. Contractor for 7-8yr starting in a hybrid program for reservists. 37 of the 40 wks. is online. I moved up to the university level where we work with the DL tools. I am part of the Academic dept. technology dept.

Task 5(b) Interview Overview
How would the DoD moving to a consolidated cloud effect your organization? What considerations are (or would you be) you worried about?
I personally love it and it makes sense and how it should be. They should consolidate the things they are doing in the military schools.
USA Learning scares us because we've had such a bad experience. Moodle being an OS system and we can't touch anything with it, it's locked down and everything is a contract mod and quite a bit of $. Even for simple things like rearranging record.
PIPS ADL Task 5b Research Plan Question Overview

(373, 380)

I work as the Information Tech Chief support XXXX online division part of the XXXX development directorate. I've been doing this for 12 yrs, I'm a XXXX engineer. I've been with XXXX since inception and have done most of the architectural design for it. Prior to that I was a XXXX later Northrup Grumman for 10 yrs supporting both joint training as well as information technology. Prior to that I was in the XXXX for 20 yrs predominately in communications/intelligence, later training fields. I been doing this all told for 42 yrs. I have a development team comprised of both contractor and govt (2/3 govt 1/3 contractor mix) with the idea that contractor's adds capacity. If we lost our contracts, we could still support XXXX with basic services. My team, most are senior sw developers, combined experience in terms of yrs, in excess of 350 yrs. We've been doing this for XXXX for the last 12 yrs.
I've come into this position 18 mo ago as the Chief of the XXXX online. My background I'm a retired military officer but I was a HS teacher before I came into the XXXX, I was an instructor CO in the training squadron and then I was in the operational test environment and I came here and did a cpl of different jobs in joint training, planning and execution of events and observation of events and so I've had a lot of brick and mortar time, mentoring and on the job interface with students and now I'm in this current position in the DL side of learning. Learning has been throughout my entire career in the civilian sector

and govt sector. In XXXX, we have 3 branches/focus areas: tech side (mark), operational side (how we prioritize how we how we will provide the services that we provide), resource side (money, opp to expand). This is kind of what my role is to make sure the folks that need to do their job have the resources and advocacy that's required.

Task 5(b) Interview Overview

What are the types of DL systems that you use most often? How are these systems being modernized?
Part of the much larger network called the XXXX which was originally designed for M&S, located here at XXXX. Inside the environment holds the servers for XXXX online apps which would be traditionally called the LMS. We also have a bunch of components. Originally the LMS that we have was a product developed for XXXX by a defense contractor. In 2011 the contractor's home site was hacked and the source files were taken so of course my system is in jeopardy.
About that time the XXXX PM asked us if we could do it in-house. Since it was GOT sw, it wasn't proprietary we took that onboard. It was a huge piece of sw it had the traditional LMS, tracking that every time we made a sw change to that application it took 2 mo to test it. We adopted a component-based approach where I broke up the systems for the apps into different components that are interoperable but if I want to make a change to the reporting module for example, all I have to change is that component. All I have to test is that component, so we roll off sw changes a lot quicker than we could in the past. Part of that whole thing which we would call XXXX collectively we have a mgmt. system which includes the course player, I also do the sw development for the XXXX, XXXX in my capacity as a XXXX and our goal is to merge the sw bases here over the next several yrs so we build once and deploy twice.
Just for the LMS we use the inherent courseware player that came with the XXXX sw it used to be called, XXXX now we call it XXXX LMS. The XXXX uses Rustici but there are switches in the sw to either use rustici or inherent courseware player. We've got the LMS, we have the XXXX. The XXXX is a web based synchronous exercise staff trainer specifically designed to address gaps that were noticed in a training capability analysis of alternatives 10 yrs ago. One of the problems we have in Joint Training is we have individual training when taking online courses and by the time you roll around into an exercise you've basically spent the first wk of the exercise learning who's on the right or left and how to work as a team team. XXXX was designed fill that gap for sm group training so I could actually practice with the guys I would be working with prior to the exercise so that I could roll in and automatically know what I'm doing.
It is integrated with the LMS when you complete things in it, it goes into the database. What we call learning record store /report builder is another component. You do get credit for participating in this. We used as a precursor for many exercises supported by the XXXX worldwide.
We also have a synchronous classroom training capability similar to blackboard but it was OS the actual is SAKAI, we call it the virtual classroom (VClass), this is also integrated with the LMS. That's for XXXX training. That is also utilizing something we have from the XXXX called XXXX which provides cashing so the heavy content files of any of our XXXX apps are served up from the nearest DISA node, still comes back to the LMS 1s and Os of handling but heavy files are served as close as they can on our NIPRnet. That reduces the bandwidth coming out of the XXXX by 95% of approved speed of service.
An additional capability to that was a video streaming service, you could store videos or live streaming from an instructor. That we something we started using in conjunction with the virtual classroom so that you could see an instructor talking and you could ask questions. All of that is integrated with the LMS as well.
XXXX mobile was developed originally as an XXXX project. Developed a XXXX and that was launched in 2011 and was called the XXXX. When XXXX picked the project up we adopted it. It is a hybrid app, unclass, FOUO available for Android/Apple basically how it works is it is out there in the app store.

XXXX was a part of this effort. You take a course in XXXX on the LMS intro to mobile and at that point you get a pin which is assoc to your student profile. You download your app, there is a public facing element, when you put your pin it directs you to the LMS and confirms you can have access and you see content related to what your profile is. If you take any courses it will that across the LMS. That is our mobile component that is integrated.
We have course builder, a web based tool, that allows courseware developers to collaborate externally and internally, you still have to do video/graphic files in a separate app. It automatically puts the SCORM in there for you and then uploads directly into the database and file system that's pulled by the LMS. Report builder is heavily used by the admin of the system and allows you to pull student reports, you can't customize based on the available fields it also pulls xApi data from the virtual classroom so you can see the other elements.
The final component for app is the XXXX it's not a app it's more of a behind the scenes. It is a web service that we use to port student course completion out. We use that for reporting to the XXXX, XXXX and the XXXX uses it to port info into DEERS. We talked about doing this with the XXXX but they are doing it inside their LMS. They don't have a training mgmt. system per se. The XXXX has talked about doing this in a flat file export and putting in their XXXX but I've lost track of where we are.
Those are the apps that are on NIPR as well as the secure network SIPR all of those with the exception of XXXX comprises the whole architecture.

What challenges from the cybersecurity perspective do you run into?
What do you think is the cause for the cybersecurity challenge your organization is facing?
How do/what DoD cybersecurity policies most effect these challenges?
What internal cybersecurity protocols most effect these challenges?

Describe to me your organization's top three cybersecurity barriers/challenges impacting DL modernization. Is your LMS web based, are there additional concerns?
I would say there are no barriers per se it's a recognized need that we have to have cyber security. I don't have to provide all of the cyber security from my app out to the internet boundary myself. I don't know how familiar you are with DoD cyber security, the fact that we have DISA managing the overall defense information sys network (DISN) and you have the indiv services with their own cyber security boundaries we have, our own for the XXXX network inside of that enclave and the you have individual apps themselves. That's my responsibility to XXXX is to manage those apps as well as work with the cyber security teams for the XXXX as STIGS/patches/regulations come down from DISA. If I had to do this by myself I couldn't.
Having all of that and the over watch of cybercom and services cyber orgs for their networks helps protect us. It's a known problem for some XXXX but I would say a lot of those initiatives are handicapped by their failure of understanding of the battlespace within cyber as well as some of the parochialism in individual services and so forth. Tracking for example we send student completions to the XXXX, XXXX could pull them, DEERS and XXXX, as long as the services have their own personnel systems and their own means of tracking training it's based upon their needs under Title 10 to train soldiers. Trying to come up with a one size fits all is solution for anything is going to be problematic at the end of the day what matters are the tracking system and what goes into them, training files of the individual. This isn't a cyber challenge it's understanding the whole architecture and how those systems work and then getting the permission of the service advocate but cyber security folks when you come up with a collective technical solution. If you try to force a solution without understanding the architecture it will fail, you don't know what you're talking about. So, that tends to be a problem with some of the solutions.

xApi works well within our enclave but having a standardized approach on how you will track training across the services using this, how that all works is the key. Not necessary a cyber security issue it's understanding the information technology battlespace issue. From my perspective I don't have challenges with cyber I have to do things to protect us for cyber does that take a lot? Yes, of course it does, we have a lot of ppl trying to get in. 10 yrs ago we didn't have half the challenges. You can't ignore it for the security of the ind service member personal information, you have to chk the budget more and more. As you develop solutions you have to understand the architecture and the rules that cyber has out there of what you can and cannot do.

As we talk about DoD and CIO has policy and we have to comply what we've seen over the past cpl of years is a small percentage of our time has to go towards implementing those policy changes that's all under the rubric of cyber security. Those types of services/compliances/frequency of policy changes are going to go up in the future. As XXXX needs to manage he also has to keep an eye on how it's starting to increase the ratio of what we get done with our resources.

From a technical standpoint, we have to dedicate the right ppl that can implement those types of changes, it comes down to money/resources to pay for the expertise and the actual time for those ppl. That's time that they would be taking away to support.

Describe possible causes/root causes and their sources.

Are the causes for the described cybersecurity barrier common to other DoD Services and Organizations?
What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]?

What are three work arounds/best practices that you have identified to mitigate those cyber security challenges? Full awareness of the battlespace, my assumption is you do this on the front end.
Higher level, First it's our ppl/training. In order to touch the network here administratively you have to have security plus training, OS training relative to whatever sys your working on and vetted by whatever engineering outfit you work in the XXXX, in other words the ppl who work for XXXX. As I mention my ppl are experienced and have experience with specific Os's, operating languages and understand the best practices of those. I'm not getting some kid out of XXXX.
The XXXX controls the overall training of the personnel that touch the network, that helps us and they put down training for everyone to take. From a ppl perspective that's important element. SW best practices relative to what you're working on, database, java, middleware, that's equally important that is more the organizational level where we have to make sure the sw engineers have those requisite skills. From a sw development perspective it's a combo of those two.
Anything we design and subsequently develop, in the design phase we have to take into consideration the cyber security constraints at the very front. If you don't understand how the network works you basically run a big risk of deploying something later on that has to be significantly modified because you didn't take the constraints or the operating environments into consideration. Combo network awareness, ppl, sw itself.
Are these workarounds common to other DoD Services and Organizations?
What is the impact of the work around/best practice on your organization's ability to accomplish distributed learning modernization [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? *(For example, is it an 80% or 90% solution to your challenge.)*

Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of:
Manning
Training
Equipping

Describe how DL cybersecurity policy impacts decision-making process with regards to: Do you think this is combined?
Basically combined. We live this on a day to day basis. As cybercom identifies threats and how they do that, they can probably see the classification of this call. That in turn is pushed down to the forces and large, DoD networks, to implement fixes. The problem is as we've got a very good command and control mechanism in place but as XXXX indicated, the tooth to tail ratio has increased, tooth being rolling out functional advancements, rolling out XXXX. What ppl want to do vs what they have to do is a part of cyber security. As cyber reqs come down who's going to pay for them? If your fortunate to have a development team and we do, that forces us to do what we need to do first than what we want to do. For XXXX it's a balancing act. There have been times that we have been focused exclusively on cyber security upgrades because it's mandated. So, the issue at lg is DoD Information technology and US govt technology can come up with directives/instructions. The forces act immediately. On the policy side, it has to be understood that there is a monetary req that right now is unfunded. It comes out of hide. From a policy perspective, I'm sure they understand ok you are taking it out of hide at the expense of something. Some of that tends to be new tech or rolling some new functionality.

a. Hardware
b. Software
c. Networks
d. Cost

2. What cybersecurity challenges does your organization expect in terms of movement to cloud services?
   I understand why they want to move to the cloud. Understanding what cloud really is to an IT guy that really knows what it is, is a buzz word. Locations/resources and so forth. It easier to protect and it's also a big target. If you're in you're in. I liken it to what the military did in Pearl Harbor when we lined all the plane's wingtip to wingtip and all the ships bow to stern and then we got attacked. A decentralized approach from the military protection perspective makes sense, it's more costly. Costs drive your decision making and those are some of the risks that will happen. I look at this and think its similar, so I have concerns. Consolidating networks will help us from the perspective of efficiency, security, some financial aspects savings could be realized. We've done that J10 but I support but trying to put into 1? Maybe in 5 buckets. Putting it into 1 makes it a big target.
   - How would the DoD moving to a consolidated cloud effect your organization? What considerations are (or would you be) you worried about?

3. If you had a magic wand, and could wave it and solve one problem, what would that problem be?
   Resourcing in general but if I had a magic want, no one could hack us. A long time ago, we didn't have nearly amt of issues/adversaries that we have cropped up in the last 20 yrs, the exponential threat through any gap.

Another thing to consider unique to XXXX. Cyber security brethren would say it's cyber, some would say it's ease of use by the student. Another thing we do within XXXX at large is the content is org and displayed/accessible relative to who the individual is or the org the indiv is in, sometimes a combo. XXXX overall student audience includes your typical DoD/civil servants/dependents, civilian's doctor's/nurses, all of these I'm mentioning are compartmentalized. It includes multi-national partners (34-37) different foreign liaison officers that are in the bldg. that I'm sitting in right now. We have significant outreach to those officers. We fight as a coalition team. For example: the XXXX university uses XXXX for some of the junior officer training. They only see the courses that they need to see. The handling caveats relative to classifications in the DoD are displayed according to how you are getting into the system. For example, if you have a CAC you can see the FOUO handling caveat info with the exception of if you're a foreign national. Same thing with dependents, they can only see what they can see. In addition to that the entire defense in-depth from a technical perspective we also look from a content perspective and present the info according to who the indiv is or what the org is cleared for. You come into XXXX right now, XXXX example, the front part looks like the defense health agency LMS, the backend is XXXX. That's something that's unique to our system.

PIPS ADL Task 5b Research Plan Question Overview

(381, 382)

I'm the tech lead in the XXXX office at the XXXX supporting the XXXX essentially in participating in working groups. From our perspective, XXXX is a service provider, we don't really have any DL platforms of our own, we provide an infrastructure should any DoD components, XXXX if they want to host their apps inside XXXX infrastructure, we're able to provide infrastructure and platforms. With that they get certain benefits in other words if you're inside the enclave you get additional security protection that you might necessarily get.

I am a contractor for the govt specifically the environment that XXXX works for as a security engineer. My job is really to figure out what the hurdles are and figure out how to get around them.

Task 5(b) Interview Overview

1. What are the types of DL systems that you use most often? How are these systems being modernized? We don't really have DL platforms we provide the hosting environment/infrastructure, we don't create on our own apps.

Think of us as a XXXX similar to XXXX. We aren't identical but we do provide a similar type of infrastructure for example one XXXX service offering is called XXXX. That is a cloud hosting environment that is available to all DoD components for them to host their services. There is a charge depending on how much infrastructure or what their type of app is. If you type XXXX, this is a service that XXXX has that anyone in DoD can choose. It provides different hosting options. You only pay for what you use. I don't have a lot of details but if you need

more info I can offer that to you. It is hosted in the DoD environment. Being inside the parameter you can take advantage of the security.

2. What challenges from the cybersecurity perspective do you run into? If you can't answer from your perspective can you talk about different. Are there different environments.

   No, we follow all the given policy guidelines for bringing a project into play. Whether it's standing up an app or full server there is a set of guidelines that is set up by the CA (certifying official) and certified by the AO (authorizing official). There is whole list starting with the NIST 80053, DoD reqs for RMF, STIG review of the apps so on and so forth.

   b. What do you think is the cause for the cybersecurity challenge your organization is facing?
   c. How do/what DoD cybersecurity policies most effect these challenges?
   d. What internal cybersecurity protocols most effect these challenges?

3. Describe to me your organization's top three cybersecurity barriers/challenges impacting DL modernization. What do you think the challenges will be in 5 yrs…10yrs.. The timeline to get the accreditation processes through the hurdles that have to be met to get it signed off in a timeframe that is relevant for the warfighter that's on the front line who's trying to get an app in front of them, and the different orgs groups that want to argue about who has the approval process.

   I think the pace of technological innovation is changing so rapidly by the private sector. The DoD is having to keep up with a lot of the advancements that are taking place. We are essentially following industry. Challenge: how do you keep up? How do you design a system that can keep up with future threat? The devices are a lot different than they were 5 yrs ago. Ppl want to be able to do training on their personnel devices. How do you safeguard those?

   e. Describe possible causes/root causes and their sources.
   f. Are the causes for the described cybersecurity barrier common to other DoD Services and Organizations?
   g. What is the impact of the described barrier on your organization's ability to modernize distributed learning [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? Major

4. What are three work arounds/best practices that you have identified to mitigate those cyber security challenges? Harry-we are constantly working with senior folks. We don't talk about any specific vulnerabilities.

   Challenges we are constantly working with folks in leadership to address ways forward, products, pieces, parts, all of that comes to the table. We work through the issue to try and streamline but it's the bureaucracy is one of the biggest things.

   No, we don't talk about any vulnerability because those could become classified.

In a nutshell, it's constantly keeping your eyes and ears open to what's going on in the commercial industry, web, trying paying attention to all possible avenues that you have and pulling into some kind of synopsis that you can try and get an understanding of where it might go but there isn't a way to prepare for it in today's market.

RMF describes what orgs should use to potentially reduce their risk when it comes to operating any type of system/s they have and how to protect them from threats. This is a guide that DISA recommends to ensure they adopt a monitoring approach and they can keep up with new threats and vulnerabilities.

h. Are these workarounds common to other DoD Services and Organizations?

i. What is the impact of the work around/best practice on your organization's ability to accomplish distributed learning modernization [utilizing the following scale: 0 - no impact, 1 - minor impact, 2 - moderate impact, or 3 - major impact]? *(For example, is it an 80% or 90% solution to your challenge.)*

5. Describe your organization's main concerns (responsibilities) in DL modernization efforts in terms of: It's going to be all of them. It's the properly trained individuals that are trained to work in the environment that is constantly changing. The ability to refresh tech as it's available in the industry to keep us in the game that's going on with everyone else that can go to Lowe's or download on the web to use and practice with as well as have ppl in mgmt. understand that the amt of info that has to be looked at.
    j. Manning
    k. Training
    l. Equipping

6. Describe how DL cybersecurity policy impacts decision-making process with regards to: No
    m. Hardware
    n. Software
    o. Networks
    p. Cost

7. What cybersecurity challenges does your organization expect in terms of movement to cloud services? Our direction is to go to XXXX.

    The DoD is offering services, DISA is able to offer a cloud like hosting that is commercially available. A lot of the sw makers adopt sw as a service platform and they want to deliver these services through cloud based methods, we are providing XXXX as a way for sw vendors/manufactures to offer their service's right from the DoD infrastructure.

    - How would the DoD moving to a consolidated cloud effect your organization? What considerations are (or would you be) you worried about?

8. If you had a magic wand, and could wave it and solve one problem, what would that problem be? If there was one problem I would look at the risk management framework as a first step. you need to know what you have and know what's connecting in your network so you know how to secure it, appropriate mitigation, counter measures.

Orgs also face shortage of skilled IT/cyber sec professionals. It's not an easy problem to solve. Maybe, what orgs need to look at is maybe outsourcing security, or focus on what their core competencies are and maybe partner with other orgs and bring some economy to scale. We have the similar applications can we employ common safeguards in place and that way we can keep up with the adversary out there? There isn't enough money to go around.

From my perspective, when ppl say these are cyber obstacles, what one considers obstacles might be a capability put into place to safeguard the network.