MINUTES BOARD OF VISITORS ANNUAL MEETING February 28, 2018 Washington, DC

- 1. <u>DESIGNATED FEDERAL OFFICER'S REMARKS</u>. Colonel (COL) Mark Bieger stated for the record that the United States Military Academy (USMA) Board of Visitors (BoV or Board) operates under the authority of US Code Title 10, Section 4355. The Board is an Advisory Board subject to the Federal Advisory Committee Act.
- 2. <u>CHAIRMAN'S REMARKS</u>. Congressman Womack called the meeting to order and welcomed the members for taking the time out of their busy schedules to attend the meeting. He then reminded the members that the Board of Visitors (Board) is not in USMA's chain of command and only has an advisory role. Meetings are a way for members to gather information in an official capacity.
- 3. SUPERINTENDENT'S REMARKS. The Superintendent welcomed the members and recognized departing member, Ms. Bridget Altenburg, for her service to the Board in 2017. He also thanked Mr. Beau Walker, Congressman Womack's Chief of Staff, and Ms. Kimberly Crawford, of the Library of Congress, for their support and assistance in coordinating the meeting. Honorable Raymond Horoho, the Assistant Secretary of the Army for Manpower and Reserve Affairs was recognized as the Secretary of the Army's representative at the meeting. Command Sergeant Major (CSM) Timothy Guden, USMA CSM, was recognized as being selected as the next CSM for the U.S. Army Training and Doctrine Command (TRADOC). LTG Caslen noted that CSM Guden set the standard at USMA and was an exceptional role model for the Corps of Cadets, Soldiers, and the entire team. He then highlighted a few events that occurred since the last BoV meeting, which included:
- a. Army vs. Navy Football Game: Army beat Navy for a second year in a row, and because Army also beat the Air Force Academy, won the Commander In Chief trophy for the first time since 1997.
 - b. Class of 2018 celebrated 100th Night, or their last 100 days before graduation.
- c. Twelve Firsties (Seniors) earned prestigious graduate scholarships, including a Rhodes Scholar, a Marshall Scholar, three Schwartzmann Scholars, two Yenching Scholars, and three Ann Sobel Levy Scholars
- d. Distinguished visitors to West Point included Congressional delegations lead by Congressman Mike Coffman (CO), Congresswomen Jackie Speier and Norma Torres (CA), and Congresswoman Deborah Wasserman Schultz (FA). The new Secretary of the Army, Dr. Mark Esper and CIA Director, Mike Pompeo, who are both USMA graduates visited the Academy.
- 4. MR. RAYMOND HOROHO'S REMARKS. HON Horoho thanked everyone for attending and stated it was an honor to represent Secretary Esper. He then corrected his title, which is the Senior Official Performing the Duties of the Assistant Secretary of the Army. Mr. Horoho has developed an interesting relationship with USMA, as he has a nephew who is a member of USMA Class of 2021. The Secretary of the Army's number one priority is to prepare, organize, and be ready to fight and win against a different foe, and to do so in more austere environments. The Secretary of Defense's initiatives are on improving lethality, driving down

the numbers of non-deployable Soldiers, Sailors, Airmen, and Marines. The topics of leadership with character, dignity and respect tie in with the Secretary of the Army's and Defense's initiatives.

- 5. <u>ADMINISTRATIVE ANNOUNCEMENTS</u>. COL Bieger, USMA Chief of Staff, noted the last meeting of the Board of Visitors was held at West Point on October 20, 2017; a quorum was present and the Board of Visitors received updates on the following significant events since the last Board of Visitors meeting: Strategic Imperative 1- Develop Leaders of Character: Advanced Individual Development (AIAD), Semester Abroad, Military Advanced Individual Development (MIAD), Leadership Detail, Team Captain; Strategic Imperative 2 Foster Relevance and Preeminence: Build Diverse and Effective Teams, Retention trends and efforts, SHARP Education Program; Faculty and Staff Excellence; Intellectual Capital; Stewardship: Impacts of National Defense Authorization Act, Master Facility Plan 2035, A76 law, Memorialization; Culture of Excellence; Semester Highlights.
- **6. ROLL CALL.** For the record, a quorum of the Board was present. A list of attendees, annotated to reflect members arriving late or departing early is appended to these minutes.
- 7. BOARD BUSINESS. The following Board Business was discussed and voted on:
 - a. Elections of the 2018 Chair and Vice Chair.
- (1) Congressman Steve Womack was nominated for Chair and seconded, and in a unanimous vote, elected Chair of the 2018 USMA Board of Visitors.
- (2) Ms. Sue Fulton was nominated for Vice Chair and seconded, and in a unanimous vote, elected Vice Chair of the 2018 USMA Board of Visitors.
- b. Approval of the Rules of the USMA Board of Visitors. There was a motion to approve the Rules of the Board of Visitors, which was seconded. The Rules of the USMA Board of Visitors for 2018 was approved unanimously
 - c. Presidential Appointees to the USMA Board of Visitors were sworn in
 - d. The meeting minutes from the October 20, 2017 meeting were unanimously approved.
- e. The Board was updated on the status of the 2016 Annual Report, which was completed and mailed in January 2018. The Annual Report for 2017 is being drafted.
- f. The date of the Summer USMA Board of Visitors meeting was set for Monday, July 9, 2018, with activities on Saturday and Sunday, July 7-8, 2018.

8. OTHER BOARD BUSINESS.

Open Discussion: Congressman Womack introduced LTG Robert L. Caslen, the 59th Superintendent, who discussed recent incidents that were reported in the national press, including a former Cadet, now 2nd Lieutenant stationed at Fort Drum, NY, who posed for a photo after graduation, in 2016, in his Cadet uniform wearing a t-shirt that advocated an ideology that is contrary to the US Constitution. This incident was followed by a letter from a former faculty regarding the Class of 2016 Cadet in question. Investigations have been completed, however, until the legal review and due process have occurred, the results of the findings cannot be

released or discussed. The next issue discussed revolved around letters received regarding the Army-Navy game and the Armed Forces Bowl games, when stories were published by the "Daily Beast" (an online publication) using information that had been leaked by someone with intimate knowledge about USMA. The article was about whether football players at USMA are treated differently with regards to misconduct allegations, honor violations, academics, and admissions. The Department of the Army Inspector General (IG) was invited to West Point to review these records to determine if this was the case or not. USMA worked with DAIG and made available all documents they asked to review. Additionally, they were interviewed Cadets and members of the staff & faculty during the process of their review. The results have not been finalized, once the information is available it will be shared with the Board. Finally, the SAGR (Sexual Assault and Gender Relations) report was discussed; the SAGR report is based on a survey that is conducted every other year which Cadets and Midshipmen, at the Military Service Academies, participate in.

Congressman Womack asked if there were any questions or comments regarding LTG Caslen's discussion, then commented that the timing of the "Daily Beast" story about the football players, the day before the Army-Navy Game, was interesting and wondered about the intent of the author. He then asked if the "leak" of the information violated any policies or laws, and if the leak of this information was being investigated. LTG Caslen stated the release of the athletes' information was a violation of the Privacy Act as well as other laws and was being investigated by the CID (Criminal Investigation Division).

<u>a. USMA UPDATES.</u> LTG Caslen first went over the Mission and Vision Statements as well as his priorities (slides are at Appendix B). He emphasized that leaders can be the best in their class, but if they lack character, they will fail in leadership. LTG Caslen then discussed USMA's Strategic Plan, which has two imperatives:

- (1) Imperative 1 is to develop leaders of character. Its outcomes include:
 - (a) Live honorably
 - (b) Lead honorably
 - (c) Demonstrate Excellence
- (2) Imperative 2 is to foster relevance and preeminence. Its goals include
 - (a) Build and sustain diverse and effective teams
 - (b) Develop and provide intellectual capacity
 - (c) Promote staff and faculty excellence
 - (d) Practice effective stewardship
 - (e) Instill and foster a culture of excellence and winning

Congressman Womack asked if more New York City applicants were showing up in the admissions process and if there is a cost benefit to the amount of effort that's going into New York City. COL Deborah McDonald, the Director of Admissions, stated there are cost benefits; the Admissions office is seeing an increase in interested candidates and in nominations for the

New York City area. One of USMA's biggest challenges is to inspire students to consider West Point as a college option. The second challenge is, getting the candidates to complete their files (including nomination) as the candidates are interested in the beginning, then their interest wanes. LTG Caslen noted that of the eight congressional districts in New York City, only three did not nominate anyone to West Point, which is much better than in the past. Senator Kirsten Gillibrand then noted her office has been increasing the diversity of candidates throughout New York State over the last ten years by increasing outreach to veterans and to all the cities throughout the state. Congressman Womack then asked about a program in which qualified, but un-selected, candidates to West Point's files could then be provided to the Cadet Command for ROTC scholarships. COL McDonald said that program had been in place for 15-20 years and the Admissions office provides them a list of qualified, non-select candidates every year, around the end of March.

LTG Caslen then discussed USMA's Institutional Rankings, followed by Graduate Scholarship Winners, including the First Captain, Cadet Simone Askew, a Rhodes Scholar. He then discussed competitive clubs and company athletics, as well as intramurals from last fall. Many of these teams continue beat Navy. Two club teams, the Parachute Team and Cycling (Track) are national champions.

b. Commandant of Cadets: Brigadier General (BG) Steve Gilland provided an update on the military program at USMA. He began by announcing the 2nd Brigade of the 101st Airborne Division, Ft Campbell, Kentucky, would be supporting summer training at West Point. Summer training begins on May 19, followed by graduation on May 26, and R-Day (Reception Day) is on July 2. The March Back will be on August 13, begin at Camp Buckner. He invited graduates to march back the 12 miles from Camp Buckner to West Point as well. He then highlighted Cadet Leader Development Training (CLDT), which is split between the first (Senior) and second (Junior) class Cadets. Eighty percent of first class Cadets and 20 percent of second class Cadets will be identified as future Brigade Leaders in the Corps of Cadets. Cadet Leadership Training is based on the Fort Benning phase of Ranger School; it is about 18 days long, with 13 days of continuous operations in which Cadets rotate through leadership positions in a controlling-like environments. LTG Caslen noted that Cadet Leader Development Training, at Camp Buckner, is a graduation requirement and if a Cadet fails to meet the standard, or to take the course they cannot graduate. Seventeen seniors did not meet the standard and had to retake the program; once they successfully complete the program, they will graduate later this summer.

BG Gilland highlighted summer Military Individual Advanced Development (MIAD), in which more than one thousand Cadets will receive this training. Air Assault School will be conducted at West Point, with support from the Air Assault School at Fort Campbell, Kentucky; more than 700 Cadets will go through this course and qualify with Air Assault wings. Cadets also attend Airborne School, Scuba School, HALO School (military freefall school), Sapper School (an engineering school at Fort Leonard Wood, Missouri) and multiple mountaineering schools in the US and abroad. The Sandhurst Competition will take place during the second week of April. Several USMA Cadet Companies and other countries, such as Canada and England will participate. The competition takes place over 36 hours and covers 27 miles. More than a dozen military skills will be graded, including night skills.

c. Dean of the Academic Board: BG Cindy Jebb, Dean of the Academic Board shared the Academic Program's vision statement with the Board and the thought process behind it, as well as its strategic outcomes:

- (1) Educate, train and inspire cadets to become leaders of character
- (2) Prepare the rotating military faculty to return to the operational force
- (3) Provide intellectual capital to the Army and the Nation

BG Jebb highlighted that since West Point is a ".edu" organization, it makes a natural bridge for practitioners, policymakers, and academia to come together to solve problems of national significance, and this occurs in our 26 research centers on USMA. These centers provide an opportunity to look at difficult problems in an interdisciplinary way, which provides USMA a comparative advantage to look over the horizon. When operational units give USMA tough problems, USMA has the advantage of being able to look several ridgelines to help develop solutions. USMA also works with other Army and DoD agencies to vet some projects to evaluate their operational feasibility. A few examples of this research include:

- (1) High Energy Laser
- (2) Analyzing Captured Battlefield Documents
- (3) Swarm Technology
- (4) Law of Armed Conflict Book

Spring 2018 events in the Office of the Dean included the following topics, which BG Jebb discussed briefly:

- (1) McDonald Leader Conference
- (2) West Point Author's Lunch
- (3) Dean's Book Club: Throughout the Semester
- (4) Senior Conference
- (5) Projects Day

Looking forward to the future, BG Jebb discussed some Academic Year 2018 experiments and pilot programs, including the academy schedule, budget efficiencies, conference support, human resources support, talent-management based faculty searches, facility management, and classroom configuration; future academic facility projects include the Academic Building Upgrade Program (ABUP) and the Cyber Engineering Academic Center (CEAC).

d. Athletics Update: Mr. Eugene (Boo) Corrigan, Athletic Director began by noting that he soon will start his eighth year at West Point. He discussed the mission statement of Army West Point athletics and highlighted some graduates who had been Corps Squad athletes while they attended West Point, including GEN Vincent K. Brooks, GEN Raymond A. Thomas, LTG H.R. McMaster, BG Cindy Jebb, and MAJ Anna McClaine. All of these leaders are leaders of character who excelled in their careers. In December 2017, Army beat Navy in the Army-Navy football game for the second year in a row. Because Army also beat Air Force in football, Army won the Commander-In-Chief trophy for the first time since 1997. Many of the cadet athletes are part of the Cadet Leadership, including the Command Sergeant Major, Deputy Brigade

Commander, and 2nd Regimental Commander to name a few. He highlighted Cadet Kenny Brinson, a football player, who was drawn to the leadership component of West Point. His sister is a Cadet as well.

Mr. Corrigan also updated the Board members on the Army West Point Athletic Association (AWPAA) cooperative agreement with the Army. The 2016 National Defense Authorization Act (NDAA) authorized the Army to enter into a cooperative agreement with the AWPAA, 501(c)3. He briefed the members on the following:

- (1) Cooperative Agreement interim/annual reporting requirements
- (2) AWPAA audited financial statement and single audit
- (3) ODIA (Office of the Directorate of Intercollegiate Athletics) NCAA (National Collegiate Athletic Association) Revenue and Expense reporting
 - (4) AWPAA NCAA Paid Ticket Attendance Audit
 - (5) Army Athletic Association continuing multiple annual financial audits
- e. Defense Health Agency. The 2017 NDAA authorized the transition of all Army hospitals to the Defense Health Agency (DHA), which will happen over a period of time. The DHA will directly affect Keller Army Community Hospital (KACH) at West Point. Based on initial reviews of KACH and its inpatient care, and a review of USMA's mission and hospital care, the reviewers understand the importance of KACH to West Point's mission, however a decision has not yet been made. The issue at hand is, if inpatient care, particularly orthopedic care, is lost at West Point, cadet athletes would need to be seen at hospitals that are 10-15 miles in either direction, over dangerous terrain in the winter. Further, there could then be a loss of accountability of cadets who are transported outside of KACH for treatment. Loss of inpatient care would also affect service members, family members, and veterans who utilize KACH. Honorable Horoho noted the phase towards having to transition hospitals under DHA is coming up on October 1. Across all installations, there will be assessment of the relationship between DHA, the Service, Senior Mission Commander and the medical treatment facility which will look at the capabilities DHA will be responsible for. When the time comes for a review of KACH, the Superintendent will be involved in the discussions, memorandums of agreement between the DHA, the medical treatment facility and the Senior Mission Commander.
- **f. Admissions Update:** COL McDonald briefed the Board on the incoming class of 2022. Today, 28 February 2018, is file completion deadline date for the Class of 2022, so a number of files that have not been completed will be closed. She pointed out the number of obligations (letters of assurance), and those selected for civilian prep school and USMA Prep School. Currently, there are about 230 unobligated congressional vacancies and offers for those vacancies will be made within the next few weeks. After that, the class of 2022 should be completed, except for those who require medical waivers. She showed a Class Comparison chart for the classes of 2017 through 2021. A new category included in this year's class comparison was for "First Generation" admitted. Senator Jerry Moran asked if the term "First Generation" could be clarified, i.e., "first generation to attend West Point" or "first generation to attend college. COL McDonald responded the number represents the number of first generation in a family to attend college (Appendix C). A new requirement this year, for admission, is for

Cadet Candidates to videotape pull up, flexed arm hang, and pushups, which delayed completion of some files. The incoming class should be about 1,200.

- g. Diversity (Faculty): BG Cindy Jebb updated the Board on the diversity of the faculty and blend of excellence. She discussed senor civilian and military faculty, junior civilian faculty and rotating military faculty and gave statistics on gender/race, percentages of Full Professors, Associate Professors, Assistant Professors and Instructors, as well as the faculty's educational level and commissioning sources for military faculty. LTG Caslen discussed diversity initiatives including the Diversity Leadership Conference, outreach to members of Congress, and an endowment created for diversity and inclusion which was created by the Association of Graduates. On the academic side, there is now a minor in Diversity Inclusion that cadets can choose to take. For the Classes of 2020 and 2021, there is a peer tutoring program and "first year beyond" for engineering and math
- h. SHARP Update: LTG Caslen started the update on the SHARP (Sexual Harassment and Assault Response and Prevention) Program with a slide on the DoD 2016-17 Military Service Academy Annual Report, which is released every two years. Total reports of sexual assault trended upward at West Point in 2016-17. Several members of the Board had questions regarding the upward trend in reports of sexual assault, which Ms. Samantha Ross addressed. There has been nearly a 50 percent increase of reporting at USMA due to deliberate efforts. The magnitude of the increase can't necessarily be measured compared to its prevalence. The incidents are based on cadets who have identified they had incidences of sexual assault as defined by the Uniform Code of Military Justice (UCMJ), Article 20. Questions in the survey give information about Cadets' experiences of assault prior to their attending the Academy, but are not included in USMA's prevalence numbers. USMA's program has five main areas of effort; the following three were addressed at the meeting:
 - (1) Advocacy/Victim Assistance
 - (2) Investigation
 - (3) Accountability

USMA's current focus is on prevention and assessment of the effectiveness of USMA's program. Prevention of sexual assault is a relatively new field of practice and very little research exists about the kinds of programs that actually affect change. The biggest challenge is to frame a solution set that resonates with Cadets. Ms. Ross discussed the "USMA Prevention Reset", which is a new program that will help to provide Cadets with skills so they can successfully navigate relationships with respect for self and others. The program has two phases:

- (1) Phase I Change the Narrative
- (2) Phase II Meet Cadets Where They Are

Ms. Ross covered the findings of the SHARP Education Working Group, and USMA's strengths as well as areas that were "Good-to-Great." There was further discussion regarding the SHARP update, including commendations from a few members on the excellent job USMA has done in the area of prevention of sexual assault and harassment and to keep in mind, there is still a lot of work to be done in this area, but USMA is leading the way.

- **h. Initiatives and Efforts for 2018** The following topics were covered by LTG Caslen, BG Jebb, and COL Greg Boylan:
- (1) Developing Leaders of Character. LTG Caslen discussed developing leaders of character at West Point and the development of a strategy for character development. A book, titled "Developing Leaders of Character," was created when it was realized that developing character through immersion wasn't enough. Character also needs to be taught, so a syllabus and curriculum were put together. The course goal is to live honorably; the course objectives are to teach Cadets to take morally and ethically appropriate actions regardless of personal consequences; exhibit empathy and respect towards all individuals; act with proper decorum in all environments; and seek and reflect on feedback. The course is divided into four blocks (1 for each class), instruction occurs in small groups, and reflection will be a culmination of blocks of instruction.
- (2) Academy Schedule Change, Academic Year (AY) 19. LTG Caslen handed the floor to BG Cindy Jebb who discussed schedule changes for AY 2019. These changes include creating longer classes to 55-75 minutes, creating study days by consolidating academic time, maintaining Day 1/Day 2 designations, and returning to 10 minutes between classes. The reasons for this change are based on feedback, both formal and informal, surveys and assessments over the past several years. The Academy schedule lacked quality time for study, class preparation, reflection, and work on major assignments, also there was a demand for improved pedagogical flexibility. The purpose of the change was to make changes to improve pedagogy, use time more effectively during the academic day, and foster a culture of excellence and accountability during the semester. Every other Wednesday will be Dean's time; set aside for focus on academic excellence and everyone will have uninterrupted time to work on their papers, Capstone projects, etc.
- (3) Middle States Commission on Higher Education (MSCHE). USMA is currently being review for reaccreditation by MSCHE. All institutions of higher education that are legitimate must be accredited. USMA's accreditor is MSCHE. There are seven standards, with working groups for each standard. The seven standards are Mission and Goals; Ethics and Integrity; Student Learning Experience; Support of Student Learning Experience; Educational Effectiveness Assessment; Planning, Resources, and Institutional Improvement; and Governance, Leadership and Administration. BG Jebb discussed the effect of government shutdowns on the accreditation process. When the government shuts down, MSCHE must be notified, as USMA could be at risk for accreditation due to a disruption in the continuing level of resources. Government shut downs also affect the blend of excellence as much of the civilian faculty is not exempt from government shutdown. Finally, government shut down affects talent management and it's difficult to find, and retain quality civilian faculty. This issue was discussed at length by the members; Honorable Horoho reiterated the demoralizing effects government shutdowns have on the civilian workforce, which impacts their drives of engagement and their productivity.
- (4) COL Gregory Boylan, the USMA Director of Strategic Resource Planning and Integration, is responsible for "USMA 2035: The Vision and Plan." He discussed in detail the vision for USMA's facilities in the Cadet Area as well as the West Point Military Complex, which includes Camps Buckner and Natural Bridge and Range and Training areas. USMA is currently undergoing renovations to the Cadet Barracks. Between FY13 and FY18, three sets of barracks have been renovated and the newest barracks, Davis Barracks, was opened in August 2018. From now through FY22, the remaining barracks are scheduled to be renovated; currently, Pershing Barracks is under renovation. The Cadet- and Academic Building Update Program

(CBUP and ABUP) is a decade-long Army program. The Academic facilities are sorely in need of renovations to bring them to the current standards of academia. Further, there are several other administration and academic buildings that have not seen major renovation in up to 50 years.

(5) Key Upcoming Events. The Superintendent concluded by reviewingthe list of upcoming events at USMA from March through June, including his pending Change of Command, currently scheduled for June 22. The Commander-In-Chief trophy presentation is scheduled for May 2, 2018 and the Twilight Tattoo, a US Army Band Concert Series, hosted by USMA, is scheduled for 3 May 2018. LTG Caslen thanked the Board for their hospitality and the Member's Room in the Library of Congress, and most importantly, the Board's time and leadership.

9. <u>REMAINING BOARD BUSINESS</u>. None.

10. ADJOURNMENT. With no further comments, Congressman Womack adjourned the meeting at 3:45pm. This concluded the February 28, 2018 Spring Meeting of the USMA Board of Visitors.

Certified by:

JUL 0 6 2018

STEVE WOMACK US Representative

Chair, USMA Board of Visitors

DEADRA GHOSTLAW
Designated Federal Officer,
USMA Board of Visitors

ATTENDANCE ROSTER

Congressional Members:

Senator Richard Burr	Arrived 1315	Departed 1436
Senator Kirsten Gillibrand	Arrived 1324	Departed 1533
Senator Chris Murphy	Arrived 1334	Departed 1401
Senator Jerry Moran	Arrived 1401	•

Senator Jerry Moran

Congressman Steve Womack

Congresswoman Stephanie Murphy

Congressman Sean Patrick Maloney*

Congressman Mike Conaway

Departed 1340

Departed 1411

Returned 1520

Arrived 1305

Presidential Appointees:

Ms. Sue Fulton

Ms. Elizabeth McNally

Ms. Bridget Altenburg

Ms. Jane Holl Lute COL (Ret) Frederick H. Black, Sr. Departed 1425

The following members were absent:

HON Gerald McGowan

Based on the BOV attendance, a quorum was present.

Other attendees:

Mr. Raymond Horoho Senior Official Performing the Duties of the ASA(M&RA)

LTC Jason Kerr, XO ASA(M&RA)

LTC Charcillea (Charcy) Schaefer, SAFM-Bul (outgoing)

CPT Catherine (Catie) Shutters, SAFM-BUL (incoming)

MAJ Shawn Schroeder, OCLL

USMA Command and Staff Members in Attendance:

LTG Robert L. Caslen, Jr., Superintendent of the United States Military Academy

CSM Timothy Guden, USMA Command Sergeant Major

COL Mark D. Bieger, USMA Chief of Staff

COL Gregory Boylan, Superintendent's XO

MAJ Burton Eissler, Superintendent's Aide de Camp

LTC Justin Miller, Secretary of the General Staff

Ms. Deadra Ghostlaw, Assistant Secretary of the General Staff and DFO

Mr. Jeffrey Reynolds, Chief of Protocol/Alternate DFO

BG Cindy Jebb, Dean of the Academic Board

BG Steve Gilland, Commandant of Cadets (USCC)

CSM Tom Kenny, USCC Command Sergeant Major

Mr. Eugene Corrigan, Director of Intercollegiate Athletics

COL Andrew Hanson, Commander, USAG West Point

COL Erik Christiansen, Staff Judge Advocate

Ms. Lori Doughty, Academy Counsel

COL Deborah McDonald, Director of Admissions

SFC Joel Figueroa, Superintendent Communications NCO

COL Holly West, USMA G5

LTC Chevelle Thomas, Public Affairs Officer

Ms. Samantha Ross, SHARP Program Manager

Mr. Charles "Bo" Thompson, Sound Engineer

Mr. Dave Skoglund, Sound Engineer

Legislative Assistants:

Mr. Cole Lyle (SEN Burr)

Ms. Moran Banai (SEN Gillibrand)

Mr. Alec Johnson (SEN Murphy)

Mr. Will Goodwin (SEN Gillibrand)

Abbas Malik (SEN Gillibrand)

Alex Phillips (SEN Gillibrand

Mr. Beau Walker (Rep Womack)

LTC Alex Warthen (Rep Womack)

Mr. Ethan Abner (Rep Rooney

Ms. Heather Nelson (PS)

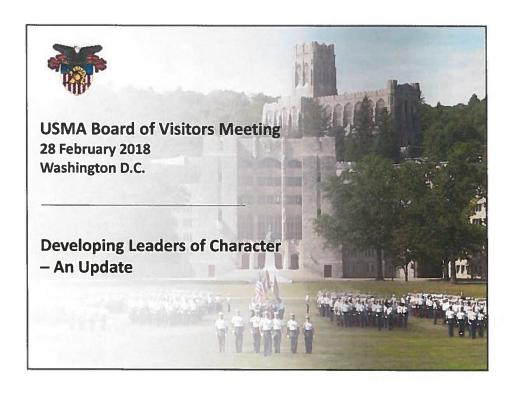
Members of the Public:

Mr. Keith McLiverty

Mr. John Anderson

Mr. George Feese

Mr. Steve Sucharski







- ☐ Status of 2016 Annual Report (mailed in January)
- ☐ Date for next meeting—9 July (morning)
- ☐ Open Discussion



Board Business





Vision and Mission

<u>Vision</u>

West Point is the preeminent leader development institution in the world.

Mission

To educate, train, and inspire the Corps of Cadets so that each graduate is a commissioned leader of character, committed to the values of Duty, Honor, Country and prepared for a career of professional excellence and service to the Nation as an officer in the United States Army.



"Inspire Leaders of Character"



USMA Strategic Plan

Commitment to Character and Excellence ...



Strategic Imperative 1: **Develop Leaders of Character** "What leaders does the Army need in 10, 20 and 30 years?"

Outcomes

Upon commissioning West Point graduates

- 1.. Live honorably:
- Lead honorably :
 Demonstrate excellence

Strategic Imperative 2: Foster Relevance and Preeminence "What is required to foster relevance and preeminence in 10, 20 and 30 years?"

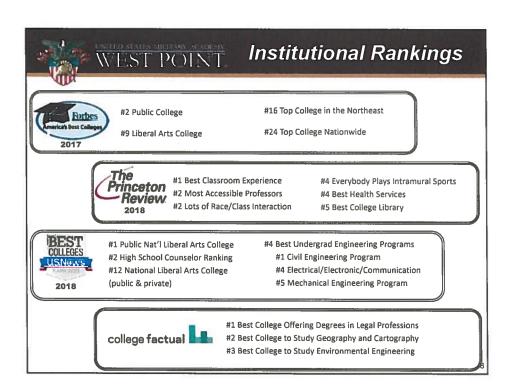
Goals

- ☐ Build and sustain diverse and effective teams
- Develop and provide intellectual capacity Promote staff and faculty excellence
- Practice effective stewardship
- Instill and foster a culture of excellence and winning



Superintendent's Priorities

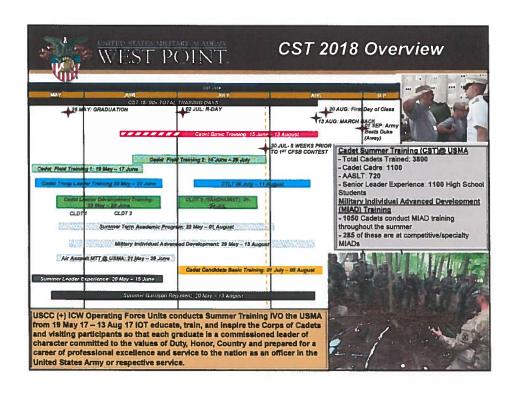
- Leader Development: Produce military leaders prepared to fight and win America's wars.
 - Honorable Living: <u>Develop leaders</u> who live honorably 24/7, who have internalized the values of Duty, Honor, Country, and the values of our Army. Ensure that climate exists here at West Point.
 - Sexual Harassment/Assault/Command Climate: <u>Develop leaders</u> who lead with command climates of dignity and respect, where everyone on the team feels value added, and feels secure both physically and emotionally. Ensure that climate exists at West Point.
 - Winning Culture: <u>Develop leaders</u> who build a culture of excellence and winning in everything we
 do. We will win honorably, not changing our standards nor who we are.
 - Diversity: <u>Develop leaders</u> who recognize and leverage the power of diverse teams. Continue to build and retain a diverse USMA team, both within the Corps of Cadets and our staff and faculty.
- Force Protection: Ensure West Point remains a safe and secure installation for the Corps of Cadets, staff and faculty and their families, and our guests.
- New York City: Continue to build our partnership with New York City to enhance Cadet development and enrich our connection with the American people.
- · Beat Navy!



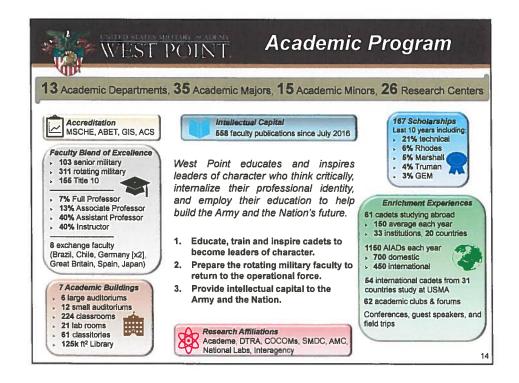
















Tomorrow's Army needs a diverse set of officers with a broad array of talents and perspectives—with deep disciplinary knowledge as well as with the agility and imagination to work across disciplines—to serve in an increasing range of specialties, from traditional branches to the newest, Cyber. How can the Academic Program best meet the challenges and exploit the opportunities of the twenty-first century as West Point approaches its 250th anniversary in 2052?

Academic Year 2018 Experiments & Pilots

- Academy Schedule
- · Budget Efficiencies
- Conference Support
- · Human Resource Specialist
- Talent-Management Based Faculty Searches
- Facility Management
- Classroom Configuration

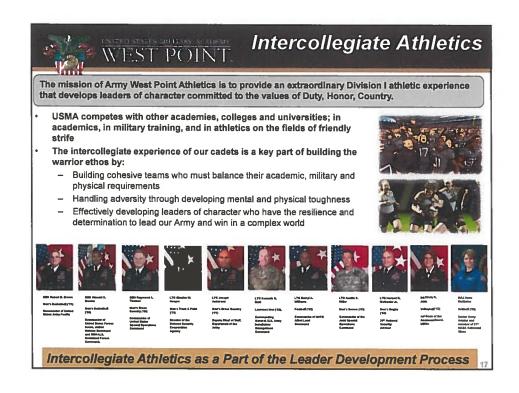
Future Academic Facilities

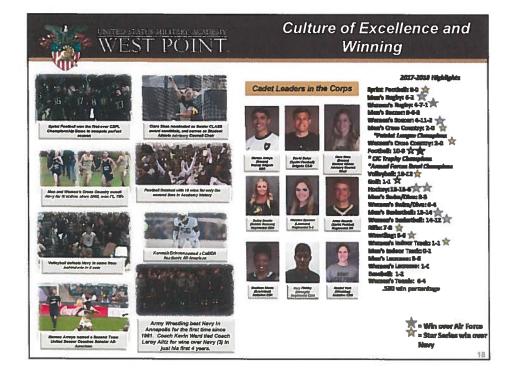
- Academic Building Upgrade Program (ABUP)
- · Cyber Engineering Academic Center (CEAC)





16







Athletic Department Financial Accountability and Auditing

- Cooperative Agreement interim/annual reporting requirements
 - First Interim Performance Report was submitted to Grants Officer on 7 November 2017.
 - Interim report annual requirement outlines execution of the intercollegiate athletics mission over the previous year, and is filed IAW the terms of the AWPAA Cooperative Agreement
 - Annual financial reports will report on activities through end of each calendar year and will be submitted via Federal Financial Report Form SF 425

AWPAA audited financial statement and single audit complete by March 30th

- Single Audit is required for most governmental recipients of federal assistance to have organization-wide financial and
 compliance audits on an annual basis. Under New York state law (7A § 172-b), a charitable organization with gross annual
 revenue over \$500,000 must file an audited financial statement prepared by an independent CPA.
- Awaiting formal results of Single Audit Act audit IAW 2 CFR 200 Subpart F and Financial Audit recently completed for initial AWPAA fiscal year

ODIA NCAA Revenue & Expense reporting complete (January every year)

- Member institutions submit financial data detailing operating revenues and expenses related to its intercollegiate athletics program to the NCAA on an annual basis. The financial data are subject to agreed-upon procedures performed by a qualified independent accountant annually for DI members. Institutions that provide data will see it populated in the NCAA Institutional Performance Program (IPP) in the spring. IPP allows institutions to not only view their data, but allows schools to compare and benchmark their data with other groups of institutions and peers.
- AWPAA NCAA Paid ticket attendance audit, NLT February 15th
 - Football Bowl Subdivision (FBS) member institutions must undertake annual certified audits verifying home football game attendance, and keep the records on hand for 4 years. FBS schools must verify compliance with the minimum attendance requirements, averaging at least 15,000 in actual or paid attendance for all home football notests over a rolling two-year period

Army Athletic Association (AAA) continues multiple annual financial audits

- In accordance with DoDI 1015.15 (Reference (d)), annual audits shall be conducted for all Non-Appropriated Fund
 Instrumentalities (NAFIs) with annual revenues or expenses exceeding \$10 million. NAFIs shall contract with a licensed Certified
 Public Accountant (CPA) firm to satisfy the financial statement audit requirement. AAA will maintain its contract with IMCOM to
 audit financial statements, conducted by outside agency (PB Mares). This report is issued in February, and it audits all material
 aspects of the financial position of AAA
- Annually conduct disinterested party inventories of the Gift Shop and Non-Appropriated Fund (NAF) fixed assets. Both

19



Foster Relevance and Preeminence

Build Diverse and Effective teams

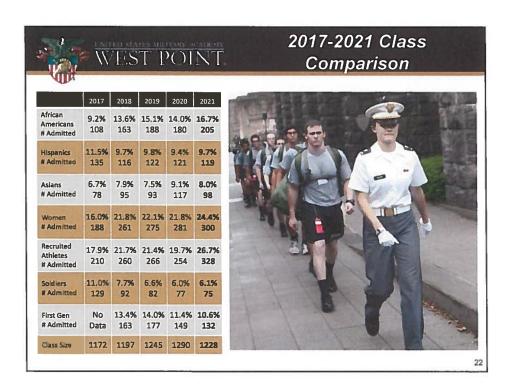


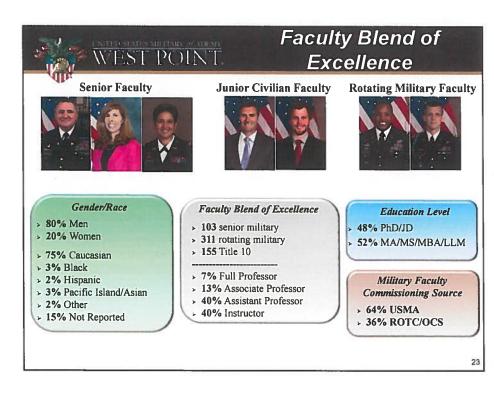


Admissions Update Class 2022									
	Total	Women	African American	Hispanic	Scholars	Leaders	Athletes	Soldiers	
Applicants	12,252	3,365	1,463	1,649	1,938	732	618	964	
Offers	732	187 (25.5%)	60 (8.2%)	75 (10.2%)	396 (54.1%)	131 (17.9%)	119 (11.0%)	21 (2.9%)	
Accepts	418	114 (27.3%)	37 (8.9%)	43 (10.3%)	190 (45.5%)	80 (19.1%)	92 (22.0%)	17 (4.1%)	
O/S LOAs	150	57	57	12	46	30	55	2	
O/S Civil Prep	3	1	0	0	0	1	1	0	
O/S USMAPS	219	46	100	10	6	26	91	49	
Obligations	1,085	286 (26.4%)	216 (19.9%)	95 (8.8%)	432 (39.8%)	182 (16.8%)	264 (24.3%)	71 (6.5%)	

As of 26 February 2018

21







Diversity Best Practices/Initiatives

Institutional

- · Established Office of Diversity, Inclusion and Equal Opportunity (Funded out of base budget)
- USMA Strategic Plan that Emphasizes Diversity and Inclusion
- Outreach to Congressional Black Caucus and Congressional Hispanic Caucus Diversity
- Leadership Conference
- New Cadet Barracks Naming: Davis Barracks
- Superintendent's Unrestricted Diversity & Inclusion Endowment
- Superintendent's Honorary ROCK of the Year Award & Honorary Tuskegee Airman

Cadet

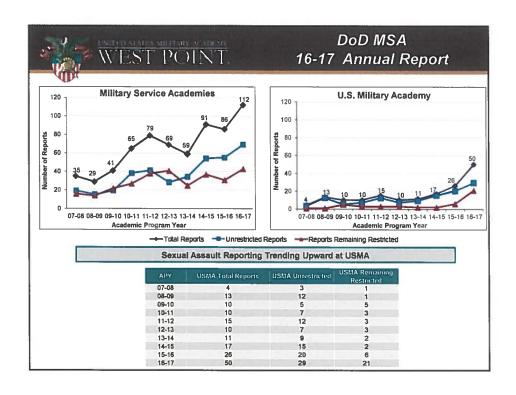
- Cadet Ambassadors/Cadet Clubs moved under ODIEO
- Diversity and Inclusion Studies Minor
- Academic clubs and forums
- Class of 2020 and 2021 retention initiatives
- Leadership, Ethics, and Diversity in STEM

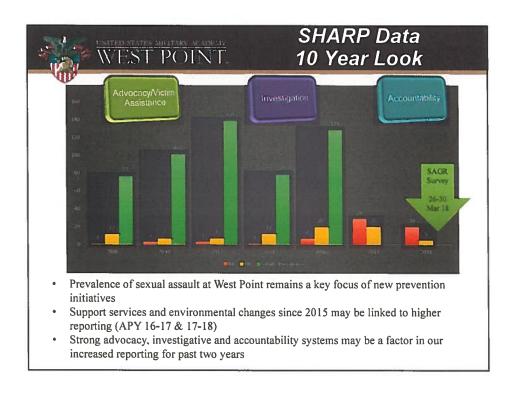
Faculty and Staff

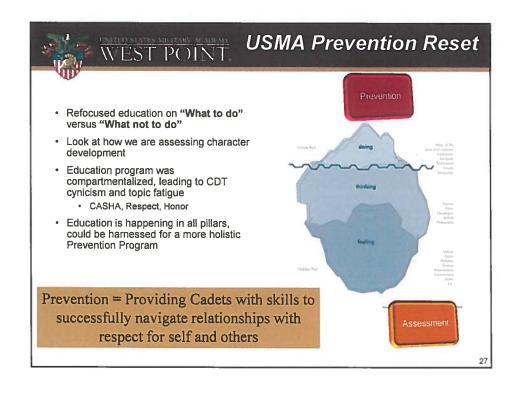
- · Georgetown University Faculty Diversity Consultation
- · HBCU Diversity Potential Faculty Talent Search
- Meetings with Human Resources command and Division commanders

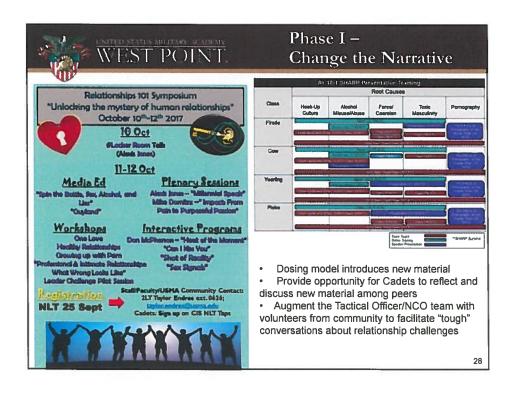
 Princeton Review: #2 Lots of Race/Class interaction

 Classes of 2020 and 2021: the most competitive and diverse classes in history of USMA with historic highs for both women and African-Americans











Phase II – Meet Cadets Where They Are

EverFi Program

- · Consultation evaluated our Prevention Program on three main areas:
 - Institutional commitment to prevention of sexual violence
 - Continuity of policies and processes to execute an effective prevention program
 - Prevention programming strengths and areas to improve
- Provide on-line training, reinforcing basic themes:
 - Sexual Violence awareness and prevention
 - Responsible alcohol use
 - Responsible and legal use of prescription medications
- Embedded surveys provide data to highlight CDT experiences, beliefs and values related to life choices (sex, alcohol and medication use)
- Real-time data allows us to address areas of concern from the surveys with meaningful interventions
 - Ex: Added a module in CCDP to explore abusive/controlling relationships, based on survey feedback
- Provides us with benchmarking data regionally and nationally

29



SHARP Education Working Group Findings

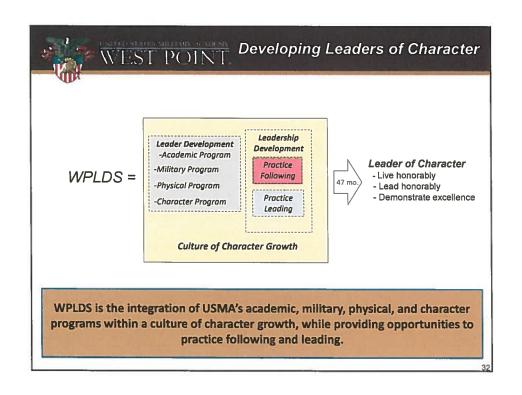
Strengths

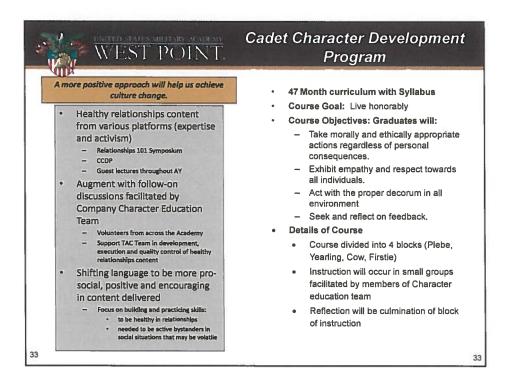
- Linked to our USMA Strategic Plan, WPLDS outcome goals, and CDS
 - Provides material that is
 - dynamic, sequential, comprehensive
 - creates conversation
 - Provides communication and confrontation skills for bystander intervention
- Leadership dimension
 - addresses individual, group, leader and organizational expectations
 - Intended to create and maintain respectful and responsible interactions
- Addresses current generational social trends and norms in a non-judgmental
- The curriculum addresses individual, relationships, community, society
- Provides knowledge and understanding about SHARP definitions, resources, and processes

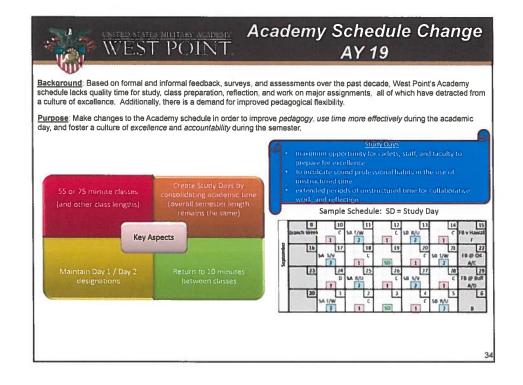
Good-to-Great

- Content needs to generate a personal connection to spark productive reflection and introspection to change beliefs and feelings
 - Tougher, more raw, candid conversations
- Behavior change/growth over 47 months can happen if content and discussion meets Cadets where they are
- Address gender related Issues without creating defensiveness, gender bias, gender bashing, etc.
 - Productively discuss personal safety and responsibility in social situations
 - Ensure discussions are candid about criminal behavior, consequences
 - Facilitate honest dialogue to expose tendencies to excuse and justify crimes
- Prep for CASHA needs to be more intentional like Ldr Challenge
 - S&F/TAC in each room
- Active involvement in the preplexecution
- Validate EO/SHARP material with SME
 - Ensure linkage to SHARP/Prevention Strategy for training, education and events











- MSCHE reaccreditation visit—Spring 2020
- The Self-study team has already been working for over 9 months.



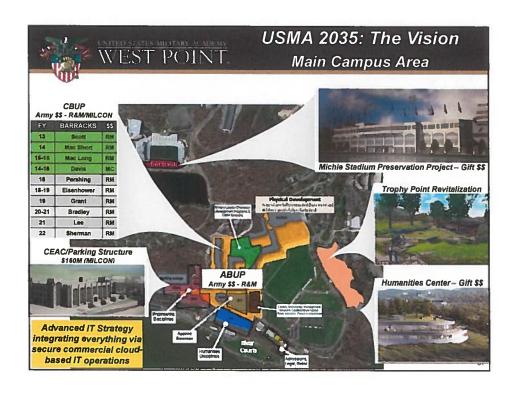
- There are 7 teams with each focused on one of the 7 standards
 - · Mission and Goals
 - · Ethics and Integrity
 - · Student Learning experience
 - · Support of Student Learning experience
 - Educational Effectiveness Assessment
 - · Planning, Resources, and Institutional Improvement
 - · Governance, Leadership and Administration
- · Team consists of approximately 75 staff and faculty
- To assist with our self-study preparation, we will host a MSCHE Vice president this spring

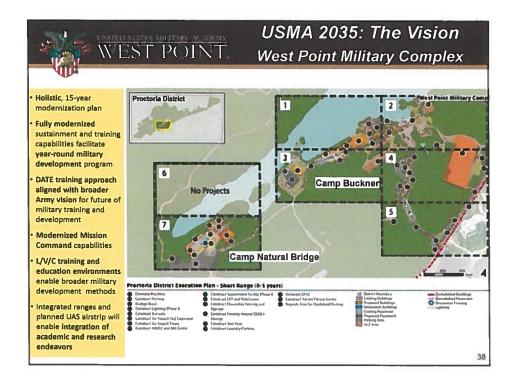
35

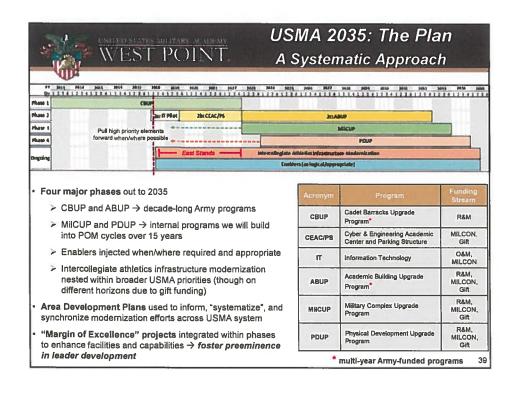


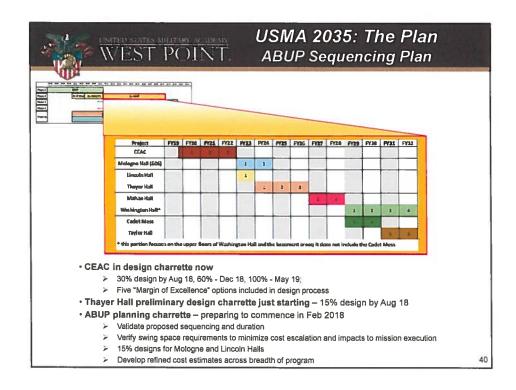
USMA 2035: The Vision and Plan

USMA G-5R













----Original Message-----

From: Bieger, Mark D COL MIL USA USMA Sent: Tuesday, March 20, 2018 8:08 AM

To: Sondheimer, Rachel M Dr. CIV USA USMA <Rachel.Sondheimer@usma.edu>; Hall, Andrew O COL MIL USA USMA <Andrew.Hall@usma.edu>; Shoop, Barry L COL MIL USA USMA <Barry.Shoop@usma.edu>; Rafferty, John L Jr LTC USARMY AWC (US)

<john.l.rafferty2.mil@mail.mil>

Cc: Jebb, Cindy BG MIL USA USMA <Cindy.Jebb@usma.edu>; Nunez, Gretchen M COL

MIL USA USMA <Gretchen.Nunez@usma.edu>; Lyle, David COL MIL USA USMA

<David.Lyle@usma.edu>; Miller, Justin L LTC MIL USA USMA

<Justin.Miller@usma.edu>; Ghostlaw, Deadra CIV USA USMA

<Deadra.Ghostlaw@usma.edu>; Schroeder, Shawn R CPT USARMY (US)

<shawn.r.schroeder.mil@mail.mil>; Kean, Charles W LTC MIL USA USMA

<Charles.Kean@usma.edu>

Subject: FW: USMA Cyber Curriculum (UNCLASSIFIED)

CLASSIFICATION: UNCLASSIFIED

Lady and Gentlemen,

Can you provide some bullets to the below RFI from OCLL (reference SecArmy O/C with SEN Gillibrand this afternoon)?

Is there an answer on how USMA is incorporating DoD's lessons learned into curriculum re: Cyber? SEN Gillibrand continued to focus on cyber efforts by asking how USMA is incorporating DoD's lessons learned into curriculum and if non-cyber-branched cadets are also trained on cyber issues

Believe we can offer some talking points that will help facilitate the discussion.

Please reply to all - and SGS will consolidate for us.

Vr Mark

COL Mark Bieger Chief of Staff, United States Military Academy West Point, NY 10996 Office: 845-938-3419

Cell: 845-527-7668 mark.bieger@usma.edu

----Original Message-----

From: Schroeder, Shawn R MAJ USARMY HQDA OCLL (US)

[mailto:shawn.r.schroeder.mil@mail.mil] Sent: Tuesday, March 20, 2018 8:04 AM To: Miller, Justin L LTC MIL USA USMA <Justin.Miller@usma.edu>; Ghostlaw,

Deadra CIV USA USMA < Deadra. Ghostlaw@usma.edu>

Cc: Bieger, Mark D COL MIL USA USMA <Mark.Bieger@usma.edu>; Kean, Charles W

LTC MIL USA USMA <Charles.Kean@usma.edu>

Subject: Fw: USMA Cyber Curriculum

Sir and Ma'am,

Please see below. Hot USMA RFI to support a SECARMY office call with SEN Gilliland this afternoon. The question was from the last BoV.

Shawn

Shawn R. Schroeder
Major, US Army
Legislative Liaison
Army Programs Division, Personnel Branch Pentagon 1E385
(O) 703-697-9134
(BB) 571-232-1794
Shawn.r.schroeder.mil@mail.mil
Original Message

From: Sperry, Adam M MAJ USARMY HQDA SECARMY (US)

<adam.m.sperry.mil@mail.mil>

Sent: Tuesday, March 20, 2018 4:39 AM

To: DeForest, Rebecca A MAJ USARMY HQDA OCLL (US)
Cc: Schroeder, Shawn R MAJ USARMY HQDA OCLL (US)

Subject: USMA Cyber Curriculum

Rebecca,

Reference this question below from Shawn's USMA BOV SPOTREP - is there an answer on how USMA is incorporating DoD's lessons learned into curriculum re: Cyber? Thanks so much, have an office call with her tomorrow.

-SEN Gillibrand continued to focus on cyber efforts by asking how USMA is incorporating DoD's lessons learned into curriculum and if non-cyber-branched cadets are also trained on cyber issues.

Respectfully, Adam Sperry MAJ, US Army

Legislative Assistant to The Secretary of the Army Pentagon Room 2E740

Office: 703-614-3234 BB: 571-295-0535

CLASSIFICATION: UNCLASSIFIED CLASSIFICATION: UNCLASSIFIED CLASSIFICATION: UNCLASSIFIED

Integration of the Cyber Domain at the United States Military Academy

by

Colonel Andrew O. Hall and Dr. Edward Sobiesk

Abstract:

The addition of cyber as a military domain, joining the other domains of land, sea, air, and space, necessitated an ongoing review of the inclusion of cyber in the 47 month officer development experience at the U.S. Military Academy at West Point, NY. We describe some of the most significant Academy initiatives resulting from this review, providing a case study for officer development that integrates the Cyber Domain. Inside the classroom, cyber is incorporated into general education courses, elective courses in multiple disciplines, senior capstone projects, independent study courses, multi-course tracks, a cyber minor, and several cyber-related majors. The Cyber Domain is also explored during summer military training and elsewhere outside the classroom through participation in cyber clubs, cyber-related conferences and training, summer internships across the U.S. Department of Defense and U.S. private sector, and through short temporary assignment to a U.S. Army cyber unit. Cadets have the opportunity to formally synchronize these activities as part of the U.S. Army's Cyber Leader Development Program, including a formal mentorship program and an Army Skill Identifier.

In memory of Professor Kirby, who started it all.

Introduction

"Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts...A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...." (William Gibson, Neuromancer, 1984)

Since William Gibson's use of the term cyberspace and the creation of the cyber punk genre, the word cyber has permeated all aspects of our global society. Although it would be hard to deny the need for integration of cyber into education, defining exactly what that is or what that entails is arguably still an unresolved question. Cyberspace has been elevated to a domain of warfare, and correspondingly, those of us in the national security profession must quickly identify what is required for integration of cyber into professional military education in order to enable our nations to provide for the common defense.

One current definition of cybersecurity is:

"A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation,

operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management" (Joint Task Force on Cybersecurity Education, 2017).

Teaching cybersecurity, as defined above, is an important start to looking at cyber education. However, the education of the next generation of strategists who will wield cyber as a key element of national power looks beyond the scope of this definition. With the inclusion of cyber as a domain of warfare, it is now included with the other domains of land, sea, air, and space, as an area of military responsibility (Nakasone and Lewis, 2017).

Within the warfighting perspective, cyber attack vectors are becoming a critical means of national power. Understanding the interplay across the spectrum of the diplomatic, informational, military, and economic (DIME) elements of national power requires an understanding of both the Cyber Domain and the strategic level of war. As part of this, a detailed understanding of cybersecurity is critical to reducing vulnerable attack surfaces, and knowledge at the international level of political science, law, and even economics is crucial to employing the elements of national power as a coordinated national military strategy. However, an understanding of each of these academic disciplines as needed in order to leverage cyber cannot be expected to exist in a single Soldier or scholar. This realization has led to a focus on teams to fully explore, defend, and exploit the Cyber Domain.

This paper will first provide an overview of related work involving integration of cyber into education. It will then shift to a detailed case study of the holistic multidisciplinary approach used to integrate cyber into the 47 month developmental experience cadets go through at the United States Military Academy at West Point, NY. We will describe some of the most significant cyber integration initiatives at the United States Military Academy, including extensive requirements and opportunities inside the classroom, outside the classroom, and as part of the U.S. Army's Cyber Leader Development Program.

Related Work

The primary related work for teaching cybersecurity spans computer security integrated at the program-level into computing curriculums and accreditation; programs, model curriculums, and accreditation criteria for cybersecurity as an independent discipline; exemplars involving cyber incorporated into education below the program level such as general education and elective courses; and cybersecurity training.

Professional societies for computing, including the Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), and the Association for Information Systems (AIS), have created curricular guidelines for Computer Science (ACM/IEEE-CS Joint Task Force on Computing Curricula, 2013), Information Systems (ACM/AIS Joint IS Curriculum Task Force, 2010), Information Technology (ACM/IEEE-CS Task Group on Information Technology Curricula, 2017), Computer Engineering (ACM/IEEE-CS Joint Task Force on Computer Engineering Curricula, 2016), and Software Engineering (IEEE-CS /ACM Joint Task Force on

Computing Curricula, 2014). These model curriculums provide frameworks that are followed by hundreds of computing programs across the United States and internationally. Each of these model curriculums contains recommended computer security content for the associated discipline, under labels such as Information Assurance and Security, Cybersecurity, and Information Security. These computer security curricular recommendations are usually meant to be taught across the program's entire curriculum rather than in a single course. As example, the Computer Science model curriculum recommends 9 lesson hours of "concepts where the depth is unique to Information Assurance and Security" and an additional 63.5 lesson hours of Information Assurance and Security content that is "integrated into other Knowledge Areas that reflect naturally implied or specified topics with a strong role in security concepts and topics" (ACM/IEEE-CS Joint Task Force on Computing Curricula, 2013). The content for these curricular recommendations is mostly technical material that applies to the part of the curriculum being covered. Thus, an agreed upon best practice at the program level for computing disciplines is to teach cybersecurity across the entire breadth of the curriculum rather than only bolted-on to the curriculum in a single course.

Additional computing program level initiatives include the National Security Agency and the Department of Homeland Security jointly sponsoring the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program that offers designations for four-year Baccalaureate/Graduate Education (CAE-CDE), Two-Year Education (CAE2Y) and Research (CAE-R) (National Centers of Academic Excellence in Cyber Defense (CAE-CD), 2016). The CAE-CD program's goal is to "reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation" (National Centers of Academic Excellence in Cyber Defense (CAE-CD), 2016). Complementing this, the National Security Agency additionally sponsors the National Centers of Academic Excellence (CAE) in Cyber Operations Program (National Centers of Academic Excellence in Cyber Operations (CAE-Cyber Operations), 2016) that supports the National Initiative for Cybersecurity Education (NICE) Framework (National Initiative for Cybersecurity Education (NICE), 2017). The CAE-Cyber Operation's intent is to facilitate curriculums that meet the goal of being a "deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science (CS), computer engineering (CE), and/or electrical engineering (EE) disciplines, with extensive opportunities for hands-on applications via labs/exercises" (National Centers of Academic Excellence in Cyber Operations (CAE-Cyber Operations), 2016). Currently, there are over 200 institutions with the CAE-CD designation (National Centers of Academic Excellence in Cyber Defense (CAE-CD), 2016) and 19 institutions with the CAE-Cyber Operations designation (National Centers of Academic Excellence in Cyber Operations (CAE-Cyber Operations), 2016).

For program-level computing accreditation, ABET accredits hundreds of computing programs across in the United States and internationally. ABET has recently changed their computing accreditation criteria, and starting in the 2018-2020 time period, all computing programs seeking accreditation or reaccreditation will have to demonstrate that they have curriculum content that sufficiently covers "principles and practices for secure computing" appropriate to their discipline (ABET, CAC General and Program Criteria (Version 2.0), 2017).

From the viewpoint of cybersecurity as a distinct discipline, and not simply an aspect of a computing discipline, a Joint Task Force constructed comprehensive cybersecurity curriculum guidelines, and ABET has published and piloted draft cybersecurity program criteria. A Joint Task Force on Cybersecurity Education comprised of four professional societies (Association for Computing Machinery, IEEE Computer Society, Association for Information Systems Special Interest Group on Security, and International Federation for Information Processing Technical Committee on Information Security Education) has published Cybersecurity Curricula 2017 v.95. Its goal is, "The CSEC2017 curricular volume will be the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level" (Joint Task Force on Cybersecurity Education, 2017). The guidelines frame cybersecurity through three dimensions: crosscutting concepts, knowledge areas, and disciplinary lenses. The six crosscutting concepts are Confidentiality, Integrity, Availability, Risk, Adversarial Thinking, and Systems Thinking. The eight knowledge areas include Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security, and Societal Security. The disciplinary lenses represent "the underlying computing discipline from which the cybersecurity program was developed....The thought model encompasses the five computing disciplines identified by the ACM: computer science, computer engineering, information systems, information technology, software engineering, and a category for other disciplines such as law and medicine as well as mixed or cross disciplinary programs" (Joint Task Force on Cybersecurity Education, 2017). Based on Cybersecurity Curricula 2017 and on constituent needs, ABET has recently developed, published, and piloted cybersecurity program criteria (ABET, CAC DRAFT Cybersecurity Program Criteria, 2017).

Few institutions require cybersecurity as part of their general education program. However, some do. Examples of such requirements include mandated general education courses at the United States Military Academy (Sobiesk et al, 2015) and the United States Naval Academy (Brown et al, 2012). Examples of cyber electives and cyber minors are found in (Sobiesk et al, 2015) and (Stockman, M., Leung, S., Nyland, J., and Said, H., 2006).

Outside the classroom, there are extracurricular competitive opportunities, training courses that often have associated certifications, and government frameworks. The two most well know extracurricular cybersecurity competitions are the college-level (National Collegiate Cyber Defense Competition, 2017) that includes roughly 200 institutions and (CyberPatriot, 2017) which includes 3000+ teams composed of high school and middle school students. Additionally, hundreds of capture the flag competitions take place every year in which competitors are faced with a plethora of real world, concrete instances of computer security challenges (CTFtime.org, 2017). Hundreds of cybersecurity conferences also take place every year, providing scholars and vendors chances to share ideas, innovations, and research (InfoSec Conferences, 2017). There are numerous training courses and certifications associated specifically with cybersecurity or that include significant security components. Some of the most prominent come from organizations such as SANS (SANS, 2017), ISC2 (ISC2, 2017), Cisco (Cisco Training & Certifications, 2017), and ISACA (ISACA, 2017).

Cyber at the United States Military Academy: A Holistic Multidisciplinary Cyber Integration Methodology

The United States Military Academy (USMA) at West Point, NY has the mission to "educate, train, and inspire the Corps of Cadets so that each graduate is a commissioned leader of character." The graduates of the USMA are the officer foundation for the U.S. Army. Since 1802, when President Thomas Jefferson founded the USMA to provide America with engineers to support westward expansion, the USMA has provided the technical education needed by officers of the U.S. Army to meet the ever-changing needs of our world. Since the USMA's founding, arguably the two most significant changes to the curricula at West Point were the introduction of majors or fields of study for cadets, tailoring their program to interests and talents, and the introduction of the personal computer for each cadet in 1986.

Both locally at the USMA, and globally across the world, the personal computer combined with the network connectivity of the Internet changed the way cadets interact with every department and every discipline.

The development of computing education at the USMA has evolved from its initial roots in the Geography and Computer Science Department as Engineering Fundamentals (EF) courses to joining the Electrical Engineering and Computer Science Department as Computer Science (CS), Information Technology (IT), and Cyber (CY) courses. Computing research efforts at the USMA started with an Artificial Intelligence Research Center, which morphed to the Information Technology Operations Center (ITOC), and then eventually to the Cyber Research Center (CRC) and the Army Cyber Institute (ACI). The Cyber Research Center is focused on cadet development and faculty research in support of the Electrical Engineering and Computer Science Department's educational programs, and the Army Cyber Institute works to benefit the USMA and the U.S. Army by (1) advancing the cyber body of knowledge, (2) leveraging impactful cyber partnerships, and (3) contributing to cyber leader development processes and programs.

Just as networked personal computers necessitated many changes to the USMA's curriculum, the establishment of Cyber as the fifth domain of warfare by both the United States Department of Defense (DoD) and the North Atlantic Treaty Organization (NATO) necessitates many additional USMA education and training changes as well. It is not viewed as acceptable to only educate a subset of our leaders to understand Cyber as both a domain and element of national power. The emerging U.S. concept of Multi-Domain Battle requires all our leaders at all levels to understand operations across all five domains, including information operations and the electromagnetic spectrum. (Rhoades, Lonergan, and Hall, 2017)

In the subsequent sections, we will describe the academic program across the USMA, discussing the cyber education provided to all cadets, and then exploring the choices cadets make to deepen their exposure in order to align with their interests and goals. After discussing the academic program, we address the efforts in support of the Department of Military

Instruction and extracurricular opportunities for cadets. We tie these various programs into the USMA's instance of the U.S. Army's Cyber Leader Development Program and conclude by discussing opportunities to continue extending and enhancing the Cyber Leader Development Program across the U.S. Army's other commissioning sources.

Cyber in Core General Education Courses

During their four academic years in attendance at the USMA, all cadets must complete a minimum of 40 academic courses, of which 27 of them are core general education courses spanning a variety of disciplines, including numerous courses in the Humanities, in the Social Sciences, and in the Science, Technology, Engineering and Mathematics (STEM) disciplines. Each cadet also chooses a major from across the same spectrum, but the core STEM requirements are so rigorous that all cadets, regardless of their chosen major, receive a Bachelor of Science degree.

There are two core courses assigned to specifically introduce cadets to computing and the cyber domain. The first course, IT105 Intro to Computing and Information Technology, provides an introduction to the principles and practices of computing along with foundational design and construction techniques for computer programming. The course also covers "legal, ethical, professional, and security issues and the challenges, opportunities, and attributes of the cyber domain" (United States Military Academy, 2016). A second core course, CY305 Cyber Foundations, provides cadets the "capacity and confidence to employ information technology-hardware, software, and networks--to empower people and organizations to acquire, manage. communicate and defend information, solve problems, and adapt to change. It provides a deeper understanding of sensor and communications technologies; computer processing, storage, and networks; cyberspace operations, planning and management; interaction of IT components; IT-enabled decision making; and the evolving legal and ethical framework surrounding use of IT and operating in the cyber domain. Information Assurance issues are addressed throughout the course" (United States Military Academy, 2016). All cadets take the first course and get the content from the second course either by taking the course itself or by completing an engineering or computing major that provides equivalent content.

Several additional courses contribute to the integration of cyber across the core general education curriculum. As examples, a required Probability and Statistics course exposes cadets to scripting, command line interface, and open source software as a part of coding in the R statistical language, and required courses in International Relations, Economics, Law, and even History and Philosophy, address the evolving aspects of those disciplines that are becoming interwoven with Cyber as a Domain. All of this content is required as a part of a liberal arts education for all cadets.

In order to add depth and richness to the Academic program, the notion of threads has been added across the curriculum. The writing thread is one such example. In lieu of adding additional writing courses to the curriculum, the importance of being able to communicate in written form is reinforced by writing in most of the core program as well as in each major. This

recognizes the requirement to communicate to different audiences, as captured by writing assignments in Political Science, History, and Mathematics courses. By looking at opportunities across the 47-month experience at West Point, we work across departments to focus on critical components of the experience and capitalize on the diverse opportunities offered by our liberal arts and engineering programs.

In this spirit, the USMA is continuing to evolve the integration of cyber across the required core curriculum at West Point. Members of the USMA's faculty from many departments, including ACI faculty members, work together to integrate content and concepts involving the cyber domain without adding additional general education courses. This cooperative effort between the departments and the ACI adds to the impact of the departments and expands a cadet's exposure to the newest warfighting domain.

Cyber Engineering Track

The USMA's curriculum offers each cadet the opportunity to specialize in an engineering discipline as a part of the core program. This ensures exposure for all cadets to the engineering thought and design process. For cadets in an engineering or computing major, this engineering track experience is part of their major's required courses. The remainder of cadets, however, are required to take a three course engineering track in addition to their major. One of these three course tracks is Cyber Engineering. The Cyber Engineering Track is as follows. CY300 Programming Fundamentals covers "fundamental computing concepts that will allow them to design, build and test small to medium programs using a high-level programming language." CY350 Network Engineering and Management "addresses the analysis, design, building, and testing of modern computer networks." CY450 Cyber Security Engineering teaches cadets to "design, build and test secure networked computer systems" including a "hands-on experience with current network security tools and techniques" and a culminating exercise where cadets "design, build and test defensive measures to protect a production network from intrusions" (United States Military Academy, 2016). Essentially, the Cyber Engineering Track can be viewed as (1) code, (2) network, and (3) secure.

Cyber Minor

An emerging popular method for achieving or supplementing depth in the academic study of cyber is the Cyber Security Minor. The Cyber Minor includes a required two course Technical Track consisting of the Network Engineering and Management and the Cyber Security Engineering courses discussed above. It also requires a one course Non-Technical Track in which the cadet chooses from a policy course (IT460 Cyber Policy, Strategy & Operations), a law course (LW462 Cyber Law) or an ethics course (PY326 Cyber Ethics). The two final elective courses for the minor are selected from a number of courses across a spectrum of disciplines. A stated goal for the minor is to achieve a "balance of both technical and non-technical knowledge and skills, as well as application" (United States Military Academy, 2016). One legitimate course selection for completing the minor's requirements is to take the two required courses in the Technical Track, and then to take all three of the Non-Technical

Track options. When accounting for the additional required cyber core general education courses, this instance of the Cyber Minor provides a fairly formidable technical background along with non-technical cyber courses in policy, law, and ethics.

Cyber-Related Majors in Many Academic Disciplines

One potential approach to cyber specialization depth is to create an undergraduate Cyber major. Many institutions across the U.S., including many online programs (Best Online Cybersecurity Programs, 2017), have stood up such majors. In particular, the United States Naval Academy has a Cyber Operations major and the United States Air Force Academy has a Computer and Network Security major. As described in the Related Work section, ABET has also published and conducted pilot accreditation evaluations with draft cybersecurity program criteria that are significantly based on the *Cybersecurity Curricula 2017* guidelines published by the Joint Task Force on Cybersecurity Education.

At the USMA, the approach is to maintain the existing majors, and to allow for meaningful cyber preparation across many of them. Specifically, the USMA offers cyber-related technical major opportunities in disciplines that include Computer Science, Information Technology, Electrical Engineering, Math, Physics, and Systems Engineering. All these programs offer sequences of courses that allow students to prepare in depth for the Cyber Domain (e.g., CS's computer forensics, IT's networks and security, and EE's information assurance). These majors also integrate cyber content across the entire curriculum and all of the majors include a culminating capstone project, many of which are directly related to the Cyber Domain.

The Computer Science program continues to be an extremely popular major among cadets with interests in the Cyber Branch. The technical preparation of Computer Science prepares cadets especially well for the developer work role within the U.S. operational cyber forces. A Computer Science major's significant experiences with algorithms, programming, theory, and operating systems, coupled with a networking focus, prepares them for a role that is often akin to the skills required of a hacker.

Other cadets are more intrigued by applying and implementing Information Technology as opposed to developing their own new technology. Cadets with these interests continue to make the Information Technology major one of our most accessible and valuable majors. These abilities prepare cadets for roles as Signal Officers and Cyberspace Engineers as well as positions within the Cyber Branch. Cadets with an interest in a more traditional engineering program are drawn to Electrical and Systems Engineering, which have tighter historical linkages across the various fields of engineering. This variety within computing majors provides teammates that have learned to create, maintain, and evaluate systems with the ingenuity of a security researcher and the discipline of an engineer.

Applied Mathematics, Operations Research, Physics, and Cognitive Science all offer more flexibility for the cadets than the constrained schedule of the ABET accredited computing

or engineering major. It is easier to balance a variety of interests across formal methods, simulation, optimization, decision making, and network and data sciences, and pair it with any of the engineering tracks or the Cyber Minor. The problem-solving techniques and exposure to decision sciences include a variety of topics from abstract algebra and analysis to quantum mechanics and cryptography to computational and behavioral finance.

Balancing the technical majors are the Social Science approaches of the Political Science and Economics majors, and the unique, rigorous viewpoint of the Law major. These disciplines offer broad exposure to strategic issues and the diverse tools from game theory to strategic analysis. The breath of academic opportunities for the USMA's future cyber officers will enable them to address challenges across the spectrum, from technical network and cryptographic analysis to navigating the complex geopolitical networks of competitors and allies. This distribution of cadets with deep interest in cyber across various majors increases the integration of the Cyber Domain throughout the curriculum. Of note, a cadet who wishes to pursue a non-technical cyber-related major such as Law or Political Science, might choose to complete the Cyber Minor with courses that have a technical emphasis.

Cyber Electives

In support of the above cyber opportunities in general education, a track, a minor, and numerous majors, the USMA also offers many cyber electives as well as independent study opportunities. Electives are offered in computing disciplines, interdisciplinary domains, and noncomputing disciplines. An example elective in Computer Science is CS483 Digital Forensics. This advanced course has prerequisites of CS380 Computer Organization and CS481 Operating Systems. Digital Forensics explores "the evidence left behind when malicious activity occurs on an information system. The material in this course will build on your knowledge of Operating Systems, file formats, file system structure, computer architecture, and networking" (United States Military Academy, 2016). Another example elective is the Philosophy course PY326 Cyber Ethics. The course has a prerequisite of PY201 Philosophy and Ethical Reasoning. Cyber Ethics examines "current ethical, social and legal issues related to cyberspace, with a particular focus on: (1) the regulation or regulability of cyberspace; (2) the inherent tensions between traditional government surveillance and public safety efforts and the growing necessity for strong cyber security practices; (3) the ethical concerns surrounding government secrecy; (4) privacy and anonymization in cyberspace; and (5) cyber weapons and cyberwar" (United States Military Academy, 2016). Other popular electives include the IT460 Cyber Policy, Strategy & Operations and the LW462 Cyber Law previously discussed in the Cyber Minor section above.

In addition to the cyber electives, cadets completing a cyber-related major can also choose a cyber topic for their senior capstone design experience. A recent example of a successful cyber-related capstone project was a cadet team that designed and built a "Vulnerable Web Server application ... that packages instructional materials and pre-built virtual machines, created using Oracle VirtualBox, into interactive cybersecurity lessons" designed for non-computing high school and college students (Estes, T. et al, 2016).

Cyber Outside the Classroom

At the USMA, the cyber domain is also explored during summer military training that all cadets go through and elsewhere outside the classroom through optional cadet participation and attendance at cyber clubs, cyber-related conferences and training, summer internships across the U.S. Department of Defense and U.S. private sector, and through short temporary assignment to a U.S. Army cyber unit.

Cyber in Summer Small Unit Training

Each cadet spends a portion of their summer months participating in military training. One of these training requirements is called Cadet Leader Development Training, and it is completed the summer before either a cadet's junior or senior year at the USMA. During this training, cadets in small units go through tactical scenarios, including some involving Military Operations in Urban Terrain. Cadets experience, and must react to, several asymmetric components and unconventional challenges and opportunities that are now part of the modern battlefield. As example, during the summer of 2017, cadets conducting small unit exercises encountered commercial drones, Wi-Fi camera hacking, and the use of virtual reality goggles.

The use of commercial drones is proliferating on the modern battlefield, and cadets experience an adversary with a drone and are offered a counter-drone capability. The enemy is in an urban site and uses a drone to conduct surveillance and intelligence gathering against the small units the cadets are in. The scenario includes giving cadets the opportunity to neutralize the drone as well as dealing with the ramifications of their interactions and decisions with the drone. The exposure to commercial drones highlights both the dangers and opportunities for tactical surveillance as well the potential to create battlefield expedient countermeasures.

For the Wi-Fi hacking scenario, the enemy has networked cameras within an urban site, and cadet small unit leaders are able to utilize a cyber-enabled team to gain access to the networked cameras, thereby providing the cadet leaders with the ability to gather critical intelligence on the enemy positions and capabilities. During tactical training, certain communications channels (such as the networked cameras) are sometimes in play during the training, however, in order to maintain a primary focus on maneuver and tactics, versus purely cyber, other communication channels are often not attacked or exploited.

For exploring virtual reality, the cadet small unit leaders are able to virtually "walk through the urban terrain of their objective," experiencing it through virtual reality smartphone goggles. The goggles were created using photos and videos taken several months before summer training. The scenario describes retaking a town that had been previously held and offers the ability to virtually explore the town in a more immersive manner than offered with traditional map or photo reconnaissance. This experience allows cadets to start thinking about how the Cyber Domain can augment or even replace a physical reconnaissance. As part of this initiative, faculty members from the Behavior Sciences and Leadership Department evaluated

how the additional information available to cadets was processed and added to the leader's reconnaissance.

Overall, these small unit tactical scenarios provide a natural laboratory to explore the value of different types of intelligence and capabilities as well as the ability to incorporate elements of the Cyber Domain into training.

Cyber Clubs

There are over 100 extracurricular clubs available at the USMA. Several of these clubs are tied to cyber.

The Association for Computing Machinery Special Interest Group for Security, Audit and Control Club (SIGSAC) is open to all cadets with about 100+ participating. SIGSAC shares knowledge, cultivates technical skills, and develops leadership traits applicable to the Cyber Domain.

The Cadet Competitive Cyber Team (C3T) consists of about 20 members selected through tryouts. They practice on an almost daily basis to prepare for, and compete in, numerous capture the flag competitions that improve their own computer and network security skills and serve as a form of outreach.

The Cyber Policy Team is open to all cadets, with about 15 participating. This interdisciplinary club is dedicated to the study and application of cyber policy. The team competes at the regional, national, and international levels in various cyber policy competitions, including the annual Cyber 9/12 Student Challenge. The team's purpose is to encourage competition and a honing of cyber policy skillsets amongst our cadets.

The Amateur Radio Club (HAMS) is open to all cadets, with about 50 participating. The goal of the club is to provide an educational environment which fosters enthusiasm for amateur radio and community service.

Conferences, Training, & Internships

Several cadets attend conferences such as ShmooCon, DEF CON - Black Hat, and CyCon U.S. Attending these events allows cadets to encounter and interact with the larger cyber community of interest. In some cases, cadets even present results of their own research.

A few cadets participate in commercial cyber training with organizations such as those described in the Related Work section. Other cadets experience cyber military training by either attending a military training course or by being assigned for a few weeks to a military cyber unit.

About 100 cadets participate each summer in internships related to Computing and Electrical Engineering. All of these internships directly relate to the Cyber Domain, and many of

them are associated with conflict in the Cyber Domain. As example, about 20 cadets conduct a summer internship with the NSA. Other cadet summer internships with a cyber focus include Facebook, USAA Cyber Operations Center, FBI, CERDEC, Lincoln Laboratories, and Amazon.

A Pervasive Environment

One of the most critical aspects of a cadet's 47 month developmental experience is the conscious effort to provide the culture, environment, and role models that facilitate cadets' growth into professionals and leaders who possess the character and competence required to succeed in and adapt to the Cyber Domain and Multi-Domain Battle. This includes cadets continually interacting with members of the faculty and staff. Based on the USMA's unique mission and goals, about 25% of the faculty are civilian with the remaining 75% consisting of some of the Army's very best officers, with advanced degrees, and who represent all branches of the Army. Across this diverse and enthusiastic organization, the decision to place the Army Cyber Institute at the USMA allows for faculty with cyber expertise to be in at least eight different departments, and strongly contributes to the holistic, multidisciplinary cyber model adopted by the USMA.

The U.S. Army Cadet Cyber Development Program

USMA cadets have the opportunity to formally synchronize and track their cyber activities as part of the U.S. Army's Cyber Leader Development Program (CLDP), which includes a formal mentorship program. As described at (Army Cyber Institute, 2017), CLDP identifies, develops, and tracks cyber leaders and is encouraged for cadets taking a cyber-related majors or the cyber minor. Overall:

CLDP provides a framework for cadets to pursue 800+ hours of impactful experiences outside the classroom through internships, conferences, clubs, and seminars. Cadets in CLDP pursue opportunities to attend advanced cyber training offered by SANS, Cisco, and other organizations....Cadets in CLDP will also be favorably considered for the most challenging, technical Academic Individual Advanced Development opportunities at organizations such as the NSA, U.S. Cyber Command, U.S. Army Cyber Command, and other institutions that have a cyber operations mission. (Army Cyber Institute, 2017)

Successful completion of the Cyber Leader Development Program results in the award of an Additional Skill Identifier on a cadet's permanent military record.

Expanding Cyber to Other Commissioning Sources

The integration of cyber at the USMA encompasses pre-commissioning requirements, the academic program, and military training. Although the Cyber Leader Development Program was initially envisioned as providing a deep grounding in Cyber within this 47 month experience, it has evolved to provide experiences across a continuum, from exposure to cyber to deep technical expertise. The USMA 47 month experience provides a known baseline of knowledge

and activities for USMA cadets, however, much greater diversity exists in cyber offerings across Army Reserve Officers' Training Corps (ROTC) programs.

Currently ROTC cadets are allowed to choose from the diverse academic majors at their institution, and the Army has limited requirements concerning the academic program an ROTC cadet must choose. Therefore, the technical and cyber backgrounds of ROTC cadets varies considerably. Many U.S. Army branches of service have articulated a desire to attract STEM graduates as lieutenants, and the U.S. Army Cyber branch requires officers that are comfortable working with and solving problems as part of a highly technical Cyber team. Additionally, to excel in Multi-Domain Battle, all cadets need a technical grounding to understand the impact of the Cyber Domain on their operations.

In support of these aspirations, the Army Cyber Institute has begun expansion of the Cyber Leader Development Program to many ROTC programs. Due to the diverse resources and interest at each ROTC program location, this expansion is currently happening on almost a case-by-case basis. In support of this effort, the standards for the Cyber Leader Development Program are fully maintained, but are interpreted based on the unique circumstances of each participating ROTC cadet's program and environment. The Army also provides cyber opportunities to all ROTC cadets, such as participation in All Army Cyber Stakes, and to some ROTC cadets, such as participation in a summer internship at the NSA or at the Army Cyber Institute.

All Army Cyber Stakes is an Army-wide capture the flag type competition that offers all U.S. Army Soldiers the chance to participate in an event that allows them to demonstrate their technical cyber skills. The All Army Cyber Stakes is sponsored by the Army Cyber Institute and ForAllSecure. This past year, the competition window was 10 days and about 600 U.S. Soldiers (and cadets) participated.

The Army is also offering some ROTC cadets the chance to attend a multi-week summer cyber internship at either the NSA or the Army Cyber Institute. At the Army Cyber Institute, these cadets work on four-to-six week research projects with the faculty and staff. As examples, these ROTC cadet interns have worked on projects involving cyber law and cyber deterrence as well as setting up Apache Hadoop and Raspberry Pi clusters that perform such tasks as password cracking and Data Science calculations.

The Army Cyber Institute, in partnership with the NATO Cooperative Cyber Defence Centre of Excellence, also runs the International Conference on Cyber Conflict U.S. (CyCon U.S.). This provides a key venue for gathering the community of interest for cyber conflict. All Army Cyber Stakes winners receive their award at CyCon U.S., and ROTC cadets who participate in internships at the Army Cyber Institute sometimes present their work in poster sessions at the conference.

The Army Cyber Institute continues to expand its efforts to advise and assist the Army War College and the Joint War College's instruction and research in the Cyber domain,

incorporating these colleges' staff and students into the CyCon U.S. community and publishing their work in the Army Cyber Institute's Cyber Defense Review journal.

Conclusion

We described the ongoing efforts taking place at the USMA to teach and understand cyber in its role as a military domain. We covered some of the most significant USMA initiatives as a case study for how to holistically integrate the Cyber Domain into an officer development program. Inside the classroom, we discussed how cyber is significantly incorporated into general education courses, elective courses in multiple disciplines, senior capstone projects, independent study courses, multi-course tracks, a cyber minor, and several cyber-related majors. We also covered how the Cyber Domain is explored during summer military training and elsewhere outside the classroom through participation in cyber clubs, cyber-related conferences and training, summer internships across the U.S. Department of Defense and U.S. private sector, and through short temporary assignment to a U.S. Army cyber unit. We concluded by describing the U.S. Army's Cyber Leader Development Program that gives cadets the opportunity to formally synchronize their numerous cyber activities and to earn an Additional Skill Identifier.

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the United States Government.

References

ABET. 2017. CAC General and Program Criteria (Version 2.0). Retrieved November 12, 2017, from http://www.abet.org/abet-news/updates/

ABET. 2017. CAC *DRAFT Cybersecurity Program Criteria*. Retrieved November 12, 2017, from http://www.abet.org/abet-news/updates/

ACM/AIS Joint IS 2010 Curriculum Task Force. 2010. Curriculum Guidelines for Undergraduate Degree Programs in Information Systems. Retrieved November 12, 2017, from https://dl.acm.org/citation.cfm?id=2593310

ACM/IEEE-CS Joint Task Force on Computer Engineering Curricula. 2016. *Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering*. Retrieved November 12, 2017, from https://www.acm.org/education/curricula-recommendations

ACM/IEEE-CS Joint Task Force on Computing Curricula. 2013. *Computer Science Curricula* 2013. Retrieved November 12, 2017, from https://www.acm.org/education/curricula-recommendations

ACM/IEEE-CS Task Group on Information Technology Curricula. 2017. *Draft Curriculum Guidelines for Undergraduate Degree Programs in Information Technology*. Retrieved November 12, 2017, from http://it2017.acm.org/

Army Cyber Institute. 2017. *Cyber Leader Development Program (CLDP) Overview*. Retrieved November 24, 2017, https://www.usma.edu/acc/SitePages/CLDP.aspx

Best Online Cybersecurity Programs. 2017. Retrieved November 23, 2017, http://www.bestcolleges.com/features/top-online-bachelors-in-cybersecurity/

Brown, C. et al., 2012. *Anatomy, Dissection, and Mechanics of an Introductory Cyber-Security Course's Curriculum at the United States Naval Academy*. ACM Conference on Innovation and Technology in Computer Science Education. Haifa, Israel. Retrieved November 22, 2017, from https://dl.acm.org/citation.cfm?id=2325367

Cisco Training & Certifications. 2017. Retrieved November 22, 2017, https://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

CTFtime.org. 2017. Retrieved November 22, 2017, https://ctftime.org/

CyberPatriot. 2017. Retrieved November 22, 2017, https://www.uscyberpatriot.org/

Estes, T. et al. 2016. A Capstone Design Project for Teaching Cybersecurity to Non-technical Users. 17th Annual Conference on Information Technology Education. Boston, MA. Retrieved November 23, 2017, from https://dl.acm.org/citation.cfm?id=2978216

Hall, A.O. and Schultz, B.M. 2017. *Direct Commission for Cyberspace Specialties*, The Cyber Defense Review 2 (2), 111-124.

IEEE Computer Society/ACM Joint Task Force on Computing Curricula. 2014. *Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering*. Retrieved November 12, 2017, from https://www.acm.org/education/curricula-recommendations

InfoSec Conferences, 2017. Retrieved November 22, 2017, https://infosec-conferences.com/

ISACA. 2017. Retrieved November 22, 2017, https://www.isaca.org

ISC2. 2017. Retrieved November 22, 2017, https://www.isc2.org/

Joint Task Force on Cybersecurity Education. (2017). *Cybersecurity Curricula 2017 v. 0.75 Report*. Retrieved November 12, 2017, from https://www.csec2017.org/

Nakasone, P. M. and Lewis, C. (2017). *Cyberspace in Multi-Domain Battle. Cyber Defense Review, Vol. 2, Ed. 2.* Retrieved November 12, 2017, from http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1134630/cyberspace-in-multi-domain-battle/

National Centers of Academic Excellence in Cyber Defense (CAE-CD). 2016. *CAE-CD Program Guidance*. Retrieved November 12, 2017, from https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

National Centers of Academic Excellence in Cyber Operations (CAE-Cyber Operations). 2016. CAE-Cyber Operations Program Guidance. Retrieved November 12, 2017, from https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/

National Collegiate Cyber Defense Competition, 2017. Retrieved November 22, 2017, http://www.nationalccdc.org/

National Initiative for Cybersecurity Education (NICE). 2017. *NICE Cybersecurity Workforce Framework*. Retrieved November 12, 2017, from https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Rhoads, W.B., Lonergan, S.W., and Hall, A.O., 2017. Beyond the Keyboard: A Balanced Approach to Cyber Leader Education. forthcoming.

SANS. 2017. Retrieved November 22, 2017, https://www.sans.org/

Sobiesk, E., Blair, J., Conti, G., Lanham, M., and Taylor, H., 2015. *Cyber Education: A Multi-Level, Multi-Discipline Approach*. 16th Annual Conference on Information Technology Education. Chicago, IL. Retrieved November 12, 2017, from https://dl.acm.org/citation.cfm?id=2808038

Stockman, M., Leung, S., Nyland, J., and Said, H., 2006. *The Information Technology Minor: Filling a Need in the Workforce of Today.* 7th Annual Conference on Information Technology Education. Minneapolis, MN. Retrieved November 22, 2017, from https://dl.acm.org/citation.cfm?id=1168822

United States Military Academy. 2016. *Academic Program - Class of 2020* (RedBook). Retrieved November 23, 2017, from https://www.usma.edu/curriculum/SitePages/Course%20Catalog.aspx

Ghostlaw, Deadra CIV USA USMA

To:

Bedrin, Mark (Moran)

Cc:

Miller, Justin L LTC MIL USA USMA

Subject:

RE: [Non-DoD Source] RE: USMA Board of Visitor Meeting 28 February in Washington,

DC (best in HTML) (UNCLASSIFIED)

Mark,

The answer to Senator Moran's "first-generation" question is that neither parent nor grandparent attended college in the past. It is not "first-generation West Point," but rather "first-generation to attend college."

Deadra K. Ghostlaw
U.S. Military Academy
Assistant Secretary of the General Staff Designated Federal Officer to the
USMA Board of Visitors

COMM: (845) 938-4200 FAX: (845) 938-3214

CELL: (845) 659-0003

EMAIL: deadra.ghostlaw@usma.edu

----Original Message----

From: Bedrin, Mark (Moran) [mailto:Mark_Bedrin@moran.senate.gov]

Sent: Monday, May 7, 2018 8:51 AM

To: Ghostlaw, Deadra CIV USA USMA < Deadra. Ghostlaw@usma.edu>

Subject: RE: [Non-DoD Source] RE: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML)

(UNCLASSIFIED)

No problem at all. Thanks for the follow up!

----Original Message----

From: Ghostlaw, Deadra CIV USA USMA [mailto:Deadra.Ghostlaw@usma.edu]

Sent: Monday, May 07, 2018 8:49 AM

To: Bedrin, Mark (Moran) < Mark_Bedrin@moran.senate.gov>

Subject: RE: [Non-DoD Source] RE: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML)

(UNCLASSIFIED)

Mark,

My apologies for the delay. I was on leave when you sent this e-mail. I will get back to you as soon as I can with a response.

Respectfully,

Dede

Deadra K. Ghostlaw

U.S. Military Academy

Assistant Secretary of the General Staff Designated Federal Officer to the

USMA Board of Visitors COMM: (845) 938-4200 FAX: (845) 938-3214 CELL: (845) 659-0003

EMAIL: deadra.ghostlaw@usma.edu

----Original Message-----

From: Bedrin, Mark (Moran) [mailto:Mark_Bedrin@moran.senate.gov]

Sent: Tuesday, May 1, 2018 4:55 PM

To: Ghostlaw, Deadra CIV USA USMA < Deadra. Ghostlaw@usma.edu>

Subject: RE: [Non-DoD Source] RE: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML)

(UNCLASSIFIED)

Ma'am,

Hi, I'm looping back to this question about first generation cadets and admissions that Senator Moran asked during the last BoV meeting in February.

The answer that was given during the meeting was confusing, and I think this warrants clarification. Is there a PoC at admissions that can clarify this?

During the meeting, another member claimed this meant that they were the first in their family to attend college, not West Point specifically.

What is the stat actually measuring?

Thanks!

----Original Message-----

From: Ghostlaw, Deadra CIV USA USMA [mailto:Deadra.Ghostlaw@usma.edu]

Sent: Tuesday, February 27, 2018 1:51 PM

To: Bedrin, Mark (Moran) < Mark_Bedrin@moran.senate.gov>

Subject: RE: [Non-DoD Source] RE: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML)

(UNCLASSIFIED)

Classification: UNCLASSIFIED

Sir,

First generation of their family to attend West Point.

Respectfully,

Dede

Sent with Good (www.good.com)

From: Bedrin, Mark (Moran) < Mark_Bedrin@moran.senate.gov>

Sent: Tuesday, February 27, 2018 1:45:24 PM

To: Ghostlaw, Deadra CIV USA USMA

Subject: RE: [Non-DoD Source] RE: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML) (UNCLASSIFIED)

Dede,

I'm sorry, but that's still not clear. First Generation in what context?
First generation Americans attending? Or First generation West Pointers as in first of their family?

----Original Message----

From: Ghostlaw, Deadra CIV USA USMA [mailto:Deadra.Ghostlaw@usma.edu]

Sent: Tuesday, February 27, 2018 1:42 PM

To: Bedrin, Mark (Moran) < Mark_Bedrin@moran.senate.gov>

Subject: RE: [Non-DoD Source] RE: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML)

(UNCLASSIFIED)

Classification: UNCLASSIFIED

Mark,

It refers to first generation West Point attendees.

Thank you.

Dede

Sent with Good (www.good.com<http://www.good.com>)

From: Bedrin, Mark (Moran) < Mark_Bedrin@moran.senate.gov>

Sent: Tuesday, February 27, 2018 1:33:07 PM

To: Ghostlaw, Deadra CIV USA USMA

Subject: [Non-DoD Source] RE: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML)

(UNCLASSIFIED)

Dede.

One question- on slide 22, there is a table that lists "First Gen # Admitted". Are these first generation Americans or first generation of a family at West Point?

Thanks

----Original Message-----

From: Ghostlaw, Deadra CIV USA USMA [mailto:Deadra.Ghostlaw@usma.edu]

Sent: Monday, February 26, 2018 9:57 AM

To: Bedrin, Mark (Moran) < Mark_Bedrin@moran.senate.gov>

Subject: FW: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML) (UNCLASSIFIED)

CLASSIFICATION: UNCLASSIFIED

Mr. Bedrin,

Attached are the itinerary/agenda and slides for Wednesday's meeting. Please let me know if you have any questions.

Respectfully,

Dede

Deadra K. Ghostlaw
U.S. Military Academy
Assistant Secretary of the General Staff Designated Federal Officer to the
USMA Board of Visitors

COMM: (845) 938-4200 FAX: (845) 938-3214 CELL: (845) 659-0003

EMAIL: deadra.ghostlaw@usma.edu

```
----Original Message----
```

From: Ghostlaw, Deadra CIV USA USMA Sent: Monday, February 26, 2018 7:59 AM

To: 'Adriana Kania (adriana.kania@mail.house.gov)'

<adriana.kania@mail.house.gov>; 'Alec Johnson (alec_johnson@murphy.senate.gov)'

<alec_johnson@murphy.senate.gov>; 'ambgmcg@yahoo.com' <ambgmcg@yahoo.com>; 'Beau Walker (Rep. Womack)'

<Beau.Walker@mail.house.gov>; 'Bedrin, Mark (Moran)'

<Mark_Bedrin@moran.senate.gov>; 'Bridget Altenburg'

<baltenburg@nationalable.org>; 'Brown, Antwan D MAJ USARMY HQDA ASA MRA (US)'

<antwan.d.brown2.mil@mail.mil>; 'bsfulton80@gmail.com'

<bsfulton80@gmail.com>; 'Cantrell, Benjamin'

<Benjamin.Cantrell@mail.house.gov>; 'Caroline Ross (caroline ross@moran.senate.gov)'

<caroline_ross@moran.senate.gov>; 'Chad Sydnor (chad_sydnor@burr.senate.gov)' <chad_sydnor@burr.senate.gov>;

'Cullen Lyons (cullen.lyons@mail.house.gov)' <cullen.lyons@mail.house.gov>; 'Elizabeth McNally

(eymcnally@gmail.com)' <eymcnally@gmail.com>; 'Emily Whitfield (emily whitfield@moran.senate.gov)'

<emily_whitfield@moran.senate.gov>; 'Emily Wilson (emily_wilson@moran.senate.gov)'

<emily_wilson@moran.senate.gov>; 'Everton, Alli (Alli.Everton@mail.house.gov)' <Alli.Everton@mail.house.gov>;

Feliciano, Teresa M MAJ USARMY (US) <teresa.m.feliciano.mil@mail.mil>;

'Frederick H. Black Sr. (fhblack@nc.rr.com)' <fhblack@nc.rr.com>; 'Goodwin, Will (Gillibrand)'

<Will_Goodwin@gillibrand.senate.gov>; 'Jane Holl Lute (jhlute@gmail.com)' <jhlute@gmail.com>; 'John Laufer

(john.laufer@mail.house.gov)' <john.laufer@mail.house.gov>; 'Keener, Emily'

<Emily.Keener@mail.house.gov>; 'Kerr, Jason E LTC USARMY HQDA ASA MRA (US)'

<jason.e.kerr.mil@mail.mil>; 'Kevin Golden (kevin.golden@mail.house.gov)'

<kevin.golden@mail.house.gov>; 'Lehrer, Misha (Murphy)'

<Misha_Lehrer@murphy.senate.gov>; 'Matthew Russell (matthew.russell@mail.house.gov)'

<matthew.russell@mail.house.gov>; 'Maya Ashwal (maya_ashwal@murphy.senate.gov)'

<maya_ashwal@murphy.senate.gov>; 'Michelle.Reinshuttle@mail.house.gov' <Michelle.Reinshuttle@mail.house.gov>;

'Moore, Jessica' <Jessica.Moore@mail.house.gov>; 'Moran_banai@gillibrand.senate.gov'

<Moran_banai@gillibrand.senate.gov>;

'Ms. McNally' <elizabeth_mcnally@mckinsey.com>; 'paula morrell@mckinsey.com'

<paula_morrell@mckinsey.com>; 'Rupert, Amy A CPT USARMY HQDA ASA MRA (US)'

<amy.a.rupert.mil@mail.mil>; 'Schaefer, Charcillea A LTC USARMY HQDA ASA FM

(US) (charcillea.a.schaefer.mil@mail.mil)'

<charcillea.a.schaefer.mil@mail.mil>; 'Schroeder, Shawn R CPT USARMY HQDA OCLL (US)'

<shawn.r.schroeder.mil@mail.mil>; 'Shea, Hannah (Hannah.Shea@mail.house.gov)' <Hannah.Shea@mail.house.gov>;

'Sixbey, Mary (Gillibrand)' <Mary_Sixbey@gillibrand.senate.gov>; 'Wagner, Christine'

<Christine.Wagner@mail.house.gov>; 'Wanda Artis (Hon. Lamont)'

<wanda.artis@us.army.mil>

Subject: FW: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML) (UNCLASSIFIED)

CLASSIFICATION: UNCLASSIFIED

Dear Members, Congressional and Military Staff,

Attached are the BoV Itinerary/Agenda and slides for Wednesday's meeting at the Members Room, Library of Congress, beginning at 1:00pm.

Respectfully,

Dede

Deadra K. Ghostlaw U.S. Military Academy Assistant Secretary of the General Staff Designated Federal Officer to the **USMA Board of Visitors** COMM: (845) 938-4200

FAX: (845) 938-3214 CELL: (845) 659-0003

EMAIL: deadra.ghostlaw@usma.edu

----Original Message-----

From: Caslen, Robert LTG MIL USA USMA Sent: Sunday, February 25, 2018 2:09 PM

To: Steve Womack <saw@mail.house.gov>; mikeconawaymc@mail.house.gov; RMB@burr.senate.gov; Alec Johnson <alec_johnson@murphy.senate.gov>; Ambassador Gerald McGowan <ambgmcg@yahoo.com>; thomasjrooney@bellsouth.net; Rosen, Aimee <Aimee.Rosen@mail.house.gov>; spm18@mail.house.gov; Kevin Golden <kevin.golden@mail.house.gov>; Lehrer, Misha (Murphy) <Misha Lehrer@murphy.senate.gov>; Maya Ashwal <maya_ashwal@murphy.senate.gov>; michelle.reinshuttle@mail.house.gov;

christine.wagner@mail.house.gov; Moran Banai < Moran_banai@gillibrand.senate.gov >; Brenda Fulton <bsfulton80@gmail.com>; Ms. McNally <elizabeth_mcnally@mckinsey.com>; paula_morrell@mckinsey.com; fhblack@nc.rr.com; jhlute@gmail.com; Bridget Altenburg <bridgetaltenburg@hotmail.com>; caroline_ross@moran.senate.gov; Emily_Wilson@moran.senate.gov; Emily_Whitfield@moran.senate.gov; jack_reed@reed.senate.gov; Beau.Walker@mail.house.gov

Cc: McConville, James C MG USARMY (US) <james.c.mcconville3.mil@mail.mil>;

Cheek, Gary H MG USARMY (US) <gary.h.cheek.mil@mail.mil>; Jones, Omar J IV COL USARMY (US)

<omar.j.jones3.mil@mail.mil>; Winski, Brian E COL USARMY AWC

(US)

spian.e.winski.mil@mail.mil>; Vowell, Joel B COL USARMY AWC (US) <joel.b.vowell.mil@mail.mil>; Ryan, Joseph A COL USARMY HQDA CSA (US) <joseph.a.ryan4.mil@mail.mil>; Benchoff, Peter N COL USARMY (US)

<peter.n.benchoff.mil@mail.mil>; Rafferty, John L Jr LTC USARMY AWC (US) <john.l.rafferty2.mil@mail.mil>; Guden,

Timothy A CSM MIL USA USMA <Timothy.Guden@usma.edu>; Gilland, Steven W BG MIL USA USMA

<Steven.Gilland@usma.edu>; Jebb, Cindy BG MIL USA USMA <Cindy.Jebb@usma.edu>; Corrigan, Eugene F NAF US USA USMA <Boo.Corrigan@usma.edu>; Bieger, Mark D COL MIL USA USMA <Mark.Bieger@usma.edu>; Kean, Charles W LTC MIL USA USMA <Charles.Kean@usma.edu>; Huerter, Michail S COL MIL USA USMA <Michail.Huerter@usma.edu>;

Thomas, Chevelle LTC MIL USA USMA <Chevelle.Thomas@usma.edu>; Ghostlaw, Deadra CIV USA USMA

<Deadra.Ghostlaw@usma.edu>; Schroeder, Shawn R CPT USARMY (US) <shawn.r.schroeder.mil@mail.mil>; charcillea.a.schaefer.mil@mail.mil;

Ferrell, Monique Y Ms CIV USA AAA <monique.y.ferrell.civ@mail.mil>; Feliciano, Teresa M MAJ USARMY (US) <teresa.m.feliciano.mil@mail.mil>;

Jason.e.kerr.mil@mail.mil; anita.j.mcginthy.mil@mail.mil; wanda.l.artis.mil@mai.mil; Lorri.a.goyla.mil@mail.mil; raymond.t.horoho.civ@mail.mil; catherine.r.shutters.mil@mail.mil

Subject: USMA Board of Visitor Meeting 28 February in Washington, DC (best in HTML)

Dear Board Members,

Our Board Chair, Congressman Womack, and I are looking forward to our meeting next week in Washington DC on 28 February 2018. Thank you for making the time to come and support the Academy's mission of developing leaders of character for our Army and the Nation.

Attached is the itinerary, agenda, and current draft slide deck that we will present and discuss during the meeting. We look forward the discussions with you.

Beat Navy!

v/r

LTG Bob Caslen

Superintendent

CLASSIFICATION: UNCLASSIFIED CLASSIFICATION: UNCLASSIFIED