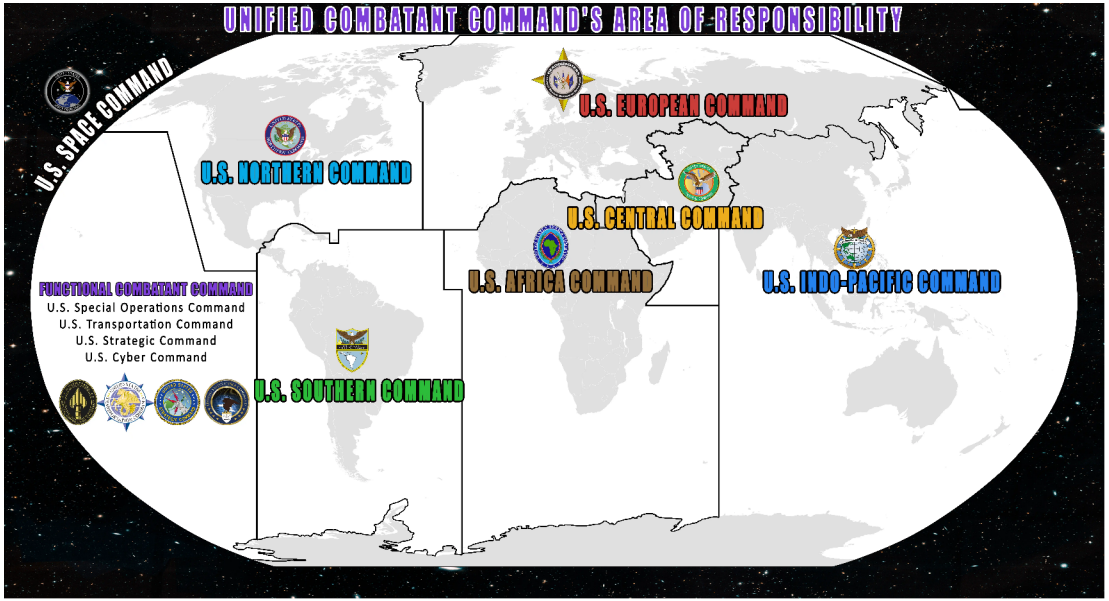
Combatant Commands

- Geographic
  - Africa Command
  - Central Command
  - European Command
  - Indo-Pacific Command
  - Northern Command
  - Southern Command
  - Space Command



Combatant Commands

- Functional
  - **Cyber Command**
  - Special Operations Command
  - Strategic Command
  - Transportation Command

U.S. Cyber Command Components

- **Joint Force Headquarters – Cyber**
- **Joint Force Headquarters – DoDIN**
- **Cyber National Mission Force**
- Army Cyber Command
- Fleet Cyber Command
- Air Forces Cyber
- Marine Corps Forces Cyberspace Command

Functional Areas

- Military units are structured along functional-area lines.
  - In staff organizations and commands, these are called directorates.

Prefix	
A	Air Force
N	Navy
M	Marine Corps
G	Army (General)
S	Army (Lower)
SOJ	Special Ops/Joint
J	Joint
C	Combined
U	United Nations
Delta	Space Force

+

Functional Area	
1	Manpower & Personnel
2	Intelligence, Surveillance and Reconnaissance
3	Operations
4	Logistics
5	Strategy, Plans, and Policy
6	Communications & Cyber
7	Training / Mission Support
8	Finance & Resources
9	Studies, Analyses, and Assessments
10	Strategic Deterrence and Nuclear Integration

Major Commands (MAJCOMS)

- Can be organized two ways: by **mission** (such as Air Combat Command or Air Education Training Command) or by **region** outside the continental United States (such as Pacific Air Forces). Major commands report directly to Air Force Headquarters.
  - Air Combat Command (ACC)
  - Air Education Training Command (AETC) (Airmen Development Command)
  - Air Force Global Strike Command (AFGSC)
  - Air Force Materiel Command (AFMC)
  - Air Force Reserve Command (AFRC)
  - Air Force Special Operations Command (AFSOC)
  - Air Mobility Command (AMC)
  - Pacific Air Forces (PACAF)
  - U.S. Air Forces Europe-Air Forces Africa (USAFE-AFAF)
  - Integrated Capabilities Command (ICC)

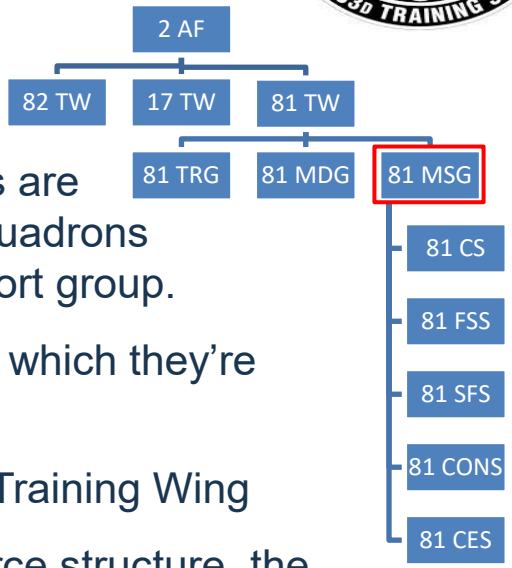
Numbered Air Force (NAF)

- A Numbered Air Force (NAF), has a more refined mission of a MAJCOM where multiple wings can fall under.
  - AETC is responsible for all Air Education Training.
    - Second Air Force is responsible for all non-pilot training.
    - Nineteenth Air Force is responsible for all Undergraduate Pilot Training

Wings

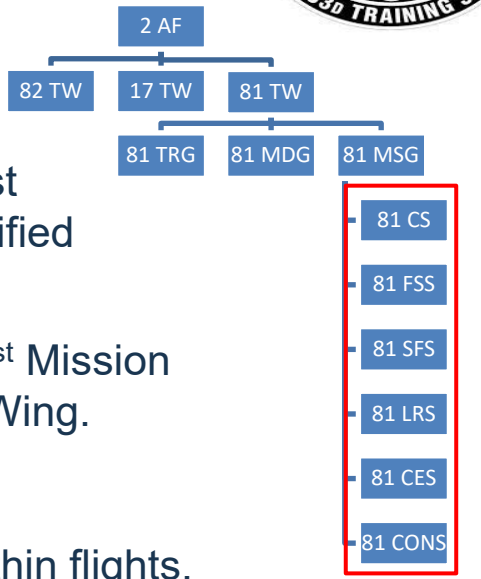
- Wings are a level of command below the NAF.
  - Comprise of two or more groups.
  - There are two types of wings: composite and objective
    - **Composite** wings operate more than one kind of aircraft and may be configured as self-contained units designated for quick air intervention anywhere in the world.
    - **Objective** wings are operational and may have a specialized mission.
    - Wings typically contain an operations group, maintenance group, support group and a medical group.

Group



- A group consists of two or more squadrons whose functions are similar to what the group is named, such as two or more squadrons supporting training functions being part of the mission support group.
  - Groups most likely take on the number of the wing to which they're assigned.
  - For instance, the 81 Training Group is part of the 81 Training Wing
  - As we work towards the lower echelons of the Air Force structure, the scope of the mission narrows.

Squadron



- Squadrons consist of two or more flights. They are the lowest level of command with a headquarters element, usually identified by the number and function.
  - The 81st Communications Squadron belongs to the 81st Mission Support Group which belongs under the 81st Training Wing.
  - Squadrons are broken into **flights**
  - Sections are formed of two or more airmen and are within flights.

Command Authority

- Combatant Command (COCOM)
- Operational Control (OPCON)
- Tactical Control (TACON)
- Support
- Administrative Control (ADCON)
- Coordinating Authority
- Direct Liaison Authorized (DIRLAUTH)

Combatant Command (COCOM)

- **Nontransferable** command authority, which **cannot be delegated**, of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command.

Operational Control (OPCON)

- Authority to perform those functions of command over subordinate forces **involving organizing and employing-commands and forces**, assigning tasks, designating objectives, and **giving authoritative direction necessary to accomplish the mission**. OPCON provides full authority to organize commands and forces and employ those forces.
- Derived from COCOM and can be delegated.
  - Ex. ANG/AFR students are OPCON to the 333 TRS but ADCON to their home unit.

Tactical Control (TACON)

- Authority over forces that is limited to the **detailed direction** and **control of movements or maneuvers** within the operational area necessary to accomplish assigned missions or **tasks.**
- Can be delegated to a lesser authority than OPCON

Support

- Exercised by commanders (at any level) to aid, assist, protect, complement, or sustain another organization or force
- It is used when neither operational control (OPCON) nor tactical control (TACON) is appropriate.
- 4 types:
  - **General Support, Mutual Support, Direct Support, Close Support**

Administrative Control (ADCON)

- Direction or exercise of authority over subordinate or other organizations with respect to administration and support
  - Ex. Guard Students go through their home units for leave and/or pay issues.

Coordinating Authority

- Commander or individual who has the **authority to require consultation between the specific functions** (ex: cyber, mobility, space) or activities involving forces of two or more Services, joint force components, or forces of the same Service or agency, but **does not have the authority to compel agreement.**

Direct Liaison Authorized (DIRLAUTH)

- Authority granted by a commander (any level) to a subordinate to directly consult or coordinate an action with a command or agency within, or outside of the granting command.
  - Ex. KAFB NIPR Outage

History of Authorities

- **1787 The Great Year**
  - The U.S. Constitution was written and signed in Philadelphia in the Assembly Room of the PA State House.
  - The convention was convened from 25 May to 17 September 1787 with the final day being the day the Constitution was signed.
  - The original Constitution is housed in the national archives in Washington D.C.
- **Why does the Constitution matter to USCYBERCOM?**
  - It is the framework of America's system of government.
  - Article 1 created the legislative branch which gives USCYBERCOM authority to operate (U.S. Code Title 10, National Defense Authorization Act, etc).
  - Article 2 created the executive branch which gives USCYBERCOM delegated presidential authority.

U.S. Codes

- Authority for cyberspace operations undertaken by the U.S. armed forces is derived from the U.S. Constitution and federal law.
- There are some key laws that apply to the DOD, specifically DOD cyberspace operations (CO).

U.S. Codes

- Title 5 Government Organization and Employee
- Title 10 Armed Forces
- Title 18 Crimes and Criminal Procedure
- Title 32 National Guard
- Title 50 War and National Defense

U.S. Codes

- Title 5 Government Organization and Employee
  - Establishes the authorities to which civil servants operate under.
- Title 10 Armed Forces
  - Outlines the role of the Armed Forces to man, train, and equip U.S. forces for military cyberspace operations.
  - Provides legal basis for the roles, missions and organization of each of the services within the DoD.

U.S. Codes

- Title 18 Crimes and Criminal Procedure
  - Outlines the role of Law Enforcement (LE) for criminal and domestic threat cyber activity.
  - FBI
  - The computer Fraud and Abuse Act is included in Title 18

U.S. Codes

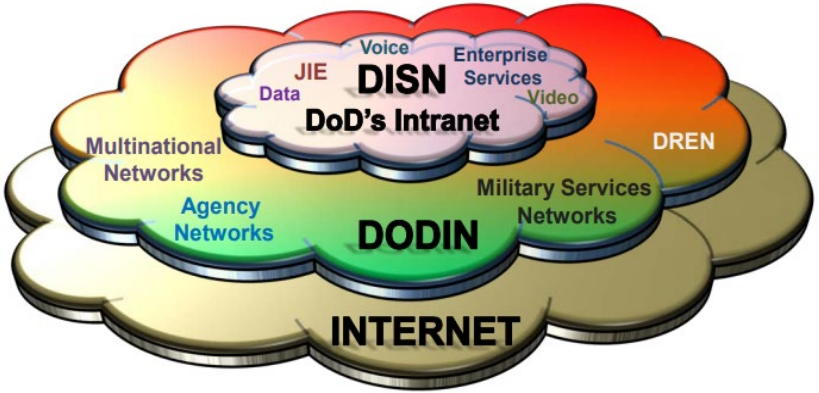
- Title 32 National Guard
  - Outlines the role of National Guard in domestic consequence management.
  - Under Title 32, National Guardsmen are controlled by the state.
  - Integrated into Title 10 when activated
    - Ex: Natural Disasters

U.S. Codes

- Title 50 War and National Defense
  - Outlines the role of war, national defense and military and foreign intelligence operations in Cyberspace.
  - Refers to intelligence agencies, activities, missions.
  - Governs intelligence agencies like the CIA or NSA.

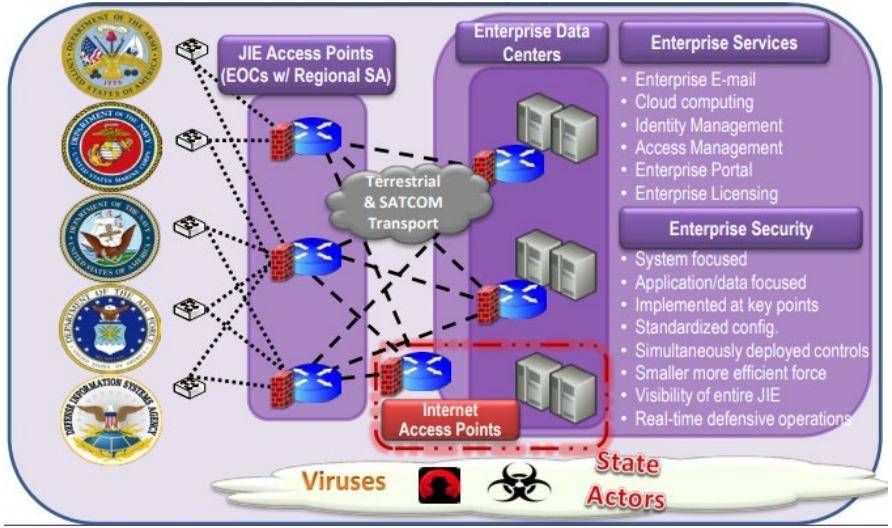
Defense Information Systems Agency (DISA)

- Implements and sustains the global network infrastructure
- Provides transport systems to support the enterprise infrastructure that allows forces to connect to information resources globally.
- Delivers Satellite Communications (SATCOM)
- Is the Department of Defense Information Network (DoDIN) backbone.
- Enables the Department of Defense's entire network (Army, Navy, Marines, Air Force)



Department of Defense Information Network

- The Department of Defense Information Network (DoDIN) is the globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating and managing information.
- Provided by the Defense Information Systems Agency (DISA)
- Each branch has a dedicated portion or domain of the DoDIN

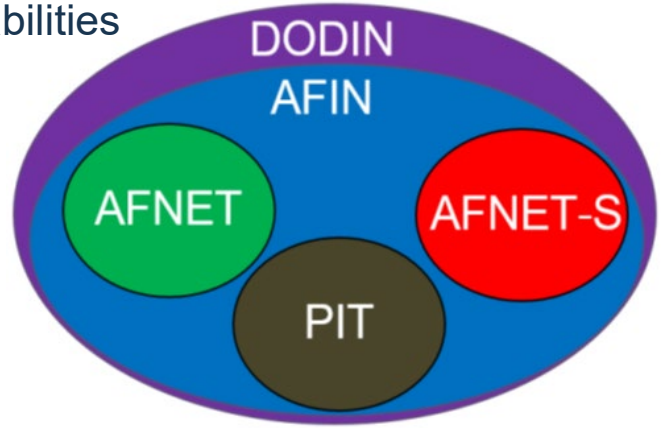


Air Force Information Network (AFIN)

- **One portion of the DoDIN**

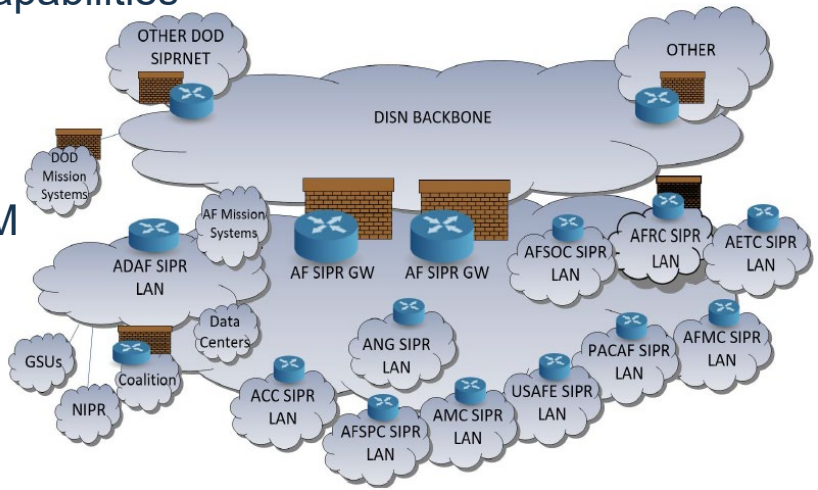
- **AFNET**
  - **Non-Secure Internet Protocol Router (NIPR)**
  - Enables unclassified Air Force operational capabilities

- Characteristics
  - Enterprise level admin privileges
  - Standardized flat design



Air Force Information Network (AFIN)

- Air Force Network (AFNET-S)
  - **Secure Internet Protocol Router (SIPR)**
  - Enables classified Air Force operational capabilities
- Characteristics
  - Architecture and funding vary by MAJCOM
  - Difficult to administer
  - No separate base network (rides AFNET)
  - Network Traffic encrypted by TACLANES



Air Force Information Network (AFIN)

- **Platform Information Technology (PIT)**
  - Special purpose systems, critical to the Air Force and mission partners
  - Not often connected to the AFNET
- Examples
  - Weapon Systems
  - Industrial Control Systems
  - Test Systems

Cyber Weapon Systems

- **Weapon System Defined:** A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.
- **Weapon System List**
  - Joint Cyber Command and Control (JCC2) **Formally C3MS**
  - Air Force Intranet Control (AFINC)
  - Cyber Security and Control System (CSCS)
  - Air Force Cyber Defense (ACD)
  - Cyberspace Defense Analysis (CDA)
  - Cyberspace Vulnerability Assessment/Hunter (CVA/H)
  - Network Attack System (NAS)

Joint Cyber Command and Control (JCC2)

- **Mission:** A USCYBERCOM-directed, joint weapon system providing overarching, interoperable, integrated 24/7 situational awareness (SA), cyber battle management and Command and Control (C2) of the DoD portion of the cyberspace domain.
- **Responsibilities:**
  - Establish, direct, coordinate cyberspace operations (OCO, DCO, and DoDIN)
  - Orders Development & Dissemination
  - Leverages SA to develop long and short-term plans, tailored strategy, course of action, and shape execution of cyberspace operations.
- **Location: 616 Operations Center (AD) – JBSA-Lackland, TX**

Air Force Intranet Control (AFINC)

- **Mission:** The Air Force Intranet Control (AFINC) Weapon System controls the flow of all external and inter-base traffic through centrally managed NIPR/SIPR gateways, Joint Regional Security Stacks (JRSS) and an inter-base Virtual Private Network (VPN) mesh.

- **Responsibilities:** Monitors and responds to anomalies in communications and information networks, information systems, and applications in coordination with DISA, MAJCOM, and the commercial sector.
  - WAN Management, DNS Management, Email Hygiene, AF Boundary Protection

- **Location: 26 NOS and 689 NOS (Reserve) – Gunter Annex, AL.**

Cyber Security and Control System (CSCS)

- **Mission:** To provide 24/7 DoDIN Ops and management functions to enable key enterprise services within Air Force unclassified and classified networks. It also supports DCO within those AF networks.
- **Responsibilities:**
  - Conducts daily activities associated with AFNET operations.
  - Provides AFNET SA
  - The final line of response for any day-to-day operational network-related issues for AF installations and MAJCOMS.
- Operators report suspicious and malicious activity to the 616 OC for enterprise correlation, assessment and de-confliction.
- CSCS crews continuously coordinate with base-level CFPs to resolve network issues.

Air Force Cyber Defense (ACD)

- **Mission:** Focused on defensive cyber operations that **prevent, detect, respond** to, and **provide forensics** of intrusions into AFIN NIPR/SIPR networks. It provides incident response along with assessing, analyzing and coordinating in the handling of security incidents and vulnerabilities.
- **Responsibilities:** Primary focuses on four main aspects of defense – prevention, detection, response and forensics.
- **Location: 33 COS (AD) – JBSA-Lackland, TX**

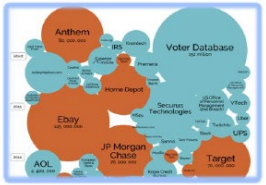
Cyberspace Defense Analysis (CDA)

- **Mission:** Provides constant monitoring for the collection, analysis and reporting of unsecured and unprotected telecommunication systems to determine if they are being used to transmit sensitive or classified information.
- **Responsibilities:** Helps organizations evaluate OPSEC and COMSEC practices and determines the amount and type of information available for adversary collection.
  - Telephony, Radio Frequency, Email, VOIP
- **Location: 33 COS (AD) – JBSA-Lackland, TX**


E-Mail


Telephony

IbC




Radio Frequency

Cyberspace Vulnerability Assessment/Hunter (CVA/H)

INTERNET

AFINC
"The Guard Dog"
External Border Protection
Routers, Firewalls, Proxies

Secured by CSCS

CDA
"The Listeners"
Prevent data Leakage

CSCS "House Security" - Internal Border Protection – Active Directory (accounts), Routers, Firewalls, Proxies

AFB

AFB

AFNET

ACD
"The Dad"
24/7 monitoring
Incident
Response/Forensics

AFB

AFB

JCC2
"The Overwatch"
Coordinates other wpn systems

CVAH

CVAH
"The Sheriff"
Threat Hunting

Cyberspace Vulnerability Assessment/Hunter (CVA/H)

- **Mission:** Used by Cyber Protection Teams (CPTs) and Mission Defense Teams (MDTs) in order to organize, train and equip to move and maneuver in cyberspace to dynamically target malicious cyber actors.
- **Responsibilities:** Designed to identify vulnerabilities and Advanced Persistent Threats (APTs) on friendly networks, information systems, and Platform Information Technology systems.
  - Data collection, Analysis & Engagement
- **Location: 92 COS (AD) & 835 COS (AD) – JBSA-Lackland, TX**
- **Location: 19 prime MDTs across various geographical locations**

Network Attack System (NAS)

- **Mission/Responsibilities:** Executes network attack planning and operations to Deny, Degrade, Disrupt and Destroy or Manipulate adversary information and information systems in support of influence operations for Component, Joint and Allied forces.
  - Precision Message Delivery (leaflet example)
  - Kinetic/Non-Kinetic effects

- **Location: 91 COS – JBSA-Lackland, TX**

DoDIN Operations

- Operations to **secure, configure, operate, extend, maintain and sustain** DoD Cyberspace
  - Preserve **Confidentiality**, **Integrity**, and **Availability**
  - **Network focused** and **threat agnostic**
  - Typically, missions are regularly scheduled, but are not considered to be routine
  - Proactive cyberspace security measures that address vulnerabilities or specific segments of the DODIN
- 16 AFCYBER/CDR, AFCYBER assures the availability of the AF portion of the DoDIN through planned and executed operations (AFIN).
- Air Force dependence on network **Confidentiality**, **Integrity**, and **Availability (CIA)** is growing as more mission essential functions, processes and systems become automated, integrated and interconnected via the AFIN.

Defense In Depth

- In order to understand and execute DiD, it's important to understand **Risk Management** and how we implement the 4 **DiD Approaches**. In doing so, it allows the Air Force to mitigate as much risk to our network as possible.
- **Risk Management** isn't just an exercise in network security philosophy. It's a part of your **DiD** that can impact technical, operational and or personnel security.
  - Measured by **Threats, Vulnerabilities** & **Impact**
    - **Threat:** Any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, other organizations, or the Nation through an information system via **unauthorized access**.
    - **Vulnerabilities:** A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.
    - **Impact:** The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, modification of information, access, loss or destruction of information and system availability.

Defense In Depth

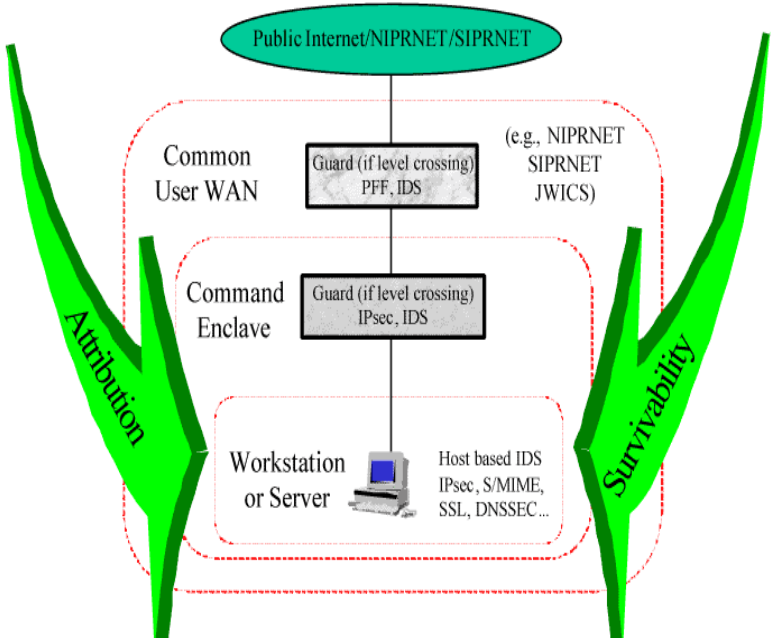
- **Remember:** DoDIN Operations consists of **A LOT** of different ways to **secure, configure, operate, extend, maintain and sustain** DoD Cyberspace.
- One way we do this is by using **Defense-In-Depth (DiD)**.
  - The DoD over the past two decades has become increasingly dependent on its computer networks which has led to an increase of attacks on DoD systems.
  - Defense in depth is an age-old military strategy and can be visualized as a castle in the middle ages. The castle didn't just depend on its wall to protect itself.
    - **It was surrounded by what?**
  - If an enemy wanted to defeat these, it'd have to take in to account all the defensive measures put in place.

Defense In Depth - Approaches

- **Defense in Depth** is an information security strategy integrating people, technology, and operation capabilities to establish variable barriers across multiple layers and missions of the organization.
- **Four DiD Approaches**
  - Uniform Protection
  - Protected Enclaves
  - Information Centric
  - Vector-Oriented

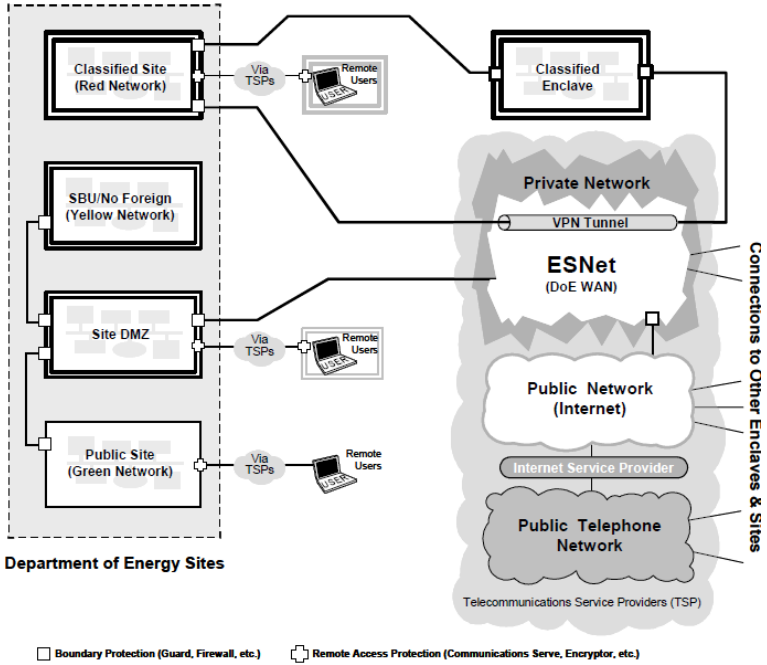
Defense In Depth – Uniform Protection

- **Uniform Protection:** Treat all systems as equally important
  - All internal hosts receive the same level of protection.
  - The most common approach



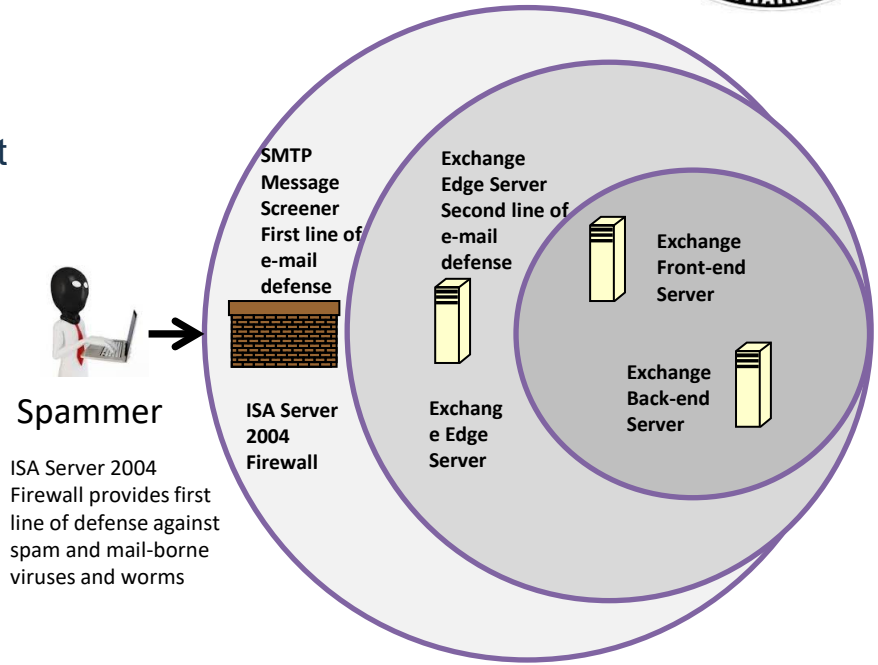
Defense In Depth – Protected Enclaves

- **Protected Enclaves:** Subdivide and separate networks.
  - VLANS
  - VPNS
  - Host Base Firewall
  - Internal Network Firewalls



Defense In Depth – Information Centric

- **Information Centric:** Prioritize protection of information over systems.
  - Identify the information you want to protect
  - Successive layers of protection between information and the attacker.



Defense In Depth – Vector Oriented

- **Vector Oriented:** ID various vectors of threats and provide security mechanisms to **prevent the use of the vector**.
  - To employ vector oriented DiD:
    - Identify the asset you want to protect.
    - Rack and stack the assets and work with the most valuable one first.
    - Brainstorm as many possible ways a threat could get to the asset.
    - Figure out how to place controls on the vectors to prevent the threat from crossing the vulnerability.

**** Which one is considered the vector of malware execution, the USB drive or the USB port? ****

Operational Reporting (OPREP)

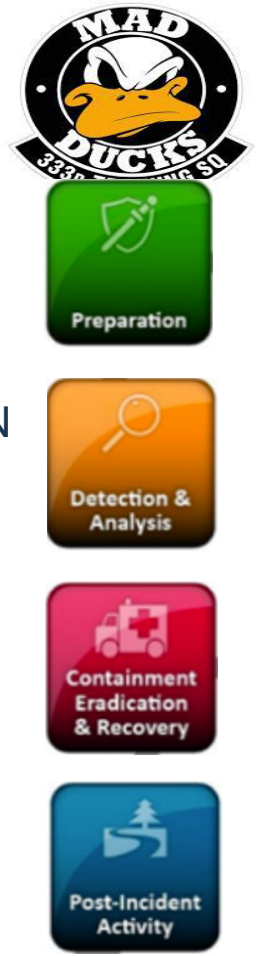
- **Concept of the OPREP System:** Provides national leaders, Chief of Staff, United States Air Force (CSAF) and Chief of Space Operations, United States Space Force intermediate commanders and their staffs the information necessary for timely operational decisions.
  - Due to the time sensitivity of OPREP information, report each event and incident promptly and as accurately as possible. The **FIRST** command post having knowledge of an event/incident will report/facilitate OPREP reporting.
  - Only Command and Control Operations Specialists and certified personnel assigned to the wing or installation command post can transmit an OPREP.
    - **Units at all levels will develop procedures to quickly obtain and report the key elements of an OPREP.**
    - The **Air Force Service Watch Cell (AFSWC)** monitors OPREPS

Operational Reports (OPREP)

- All commanders are required to release Operational Reports (OPREP) in accordance with *AFI 10-206, Operational Reporting.*
- *Various cyber events or incidents, especially those impacting mission readiness/capability, will require an OPREP.*
- ***Communications Squadrons (Cyber Events)***
  - *Commonly would report outages lasting longer than a set amount of time*
- ***The Wing Commander or Vice Wing Commander (All Events)***
  - *Reports on anything that impacts mission readiness/capability.*
  - *IE. Hurricanes, Typhoons, Major AF Accidents, Civil Misconduct, Deaths etc.*

Defensive Cyber Operations (DCO)

- **Purpose/Intent:** Defensive Cyber Operation missions are executed to **defend** the DoDIN from **active threats** in cyberspace.
- **Goals:** The main goal of DCO is to eliminate **specific threats** that have bypassed, breached, or are threatening to breach or have breached DoDIN security measures.
  - Defeat Threats
  - Preserve the ability to utilize blue cyberspace capabilities
  - Protect Data, networks, devices and other systems
  - Return a compromised network to a secure and functional state



Defensive Cyber Operation Missions

- Due to DCO's goal of defeating the threat of a specific adversary and/or to return a compromised network to a secure and functional states there are **two components** of DCO.
  - Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM)
  - Defensive Cyberspace Operations – Response Actions (DCO-RA)

Defensive Cyberspace Operations - IDM

- The form of DCO missions where authorized defense actions occur **within** the defended network or portion of cyberspace.
  - Authorized by standing order
  - Pro-active and aggressive internal threat hunting
  - Active internal countermeasures and responses to eliminate threats
  - Using specific tactics on the DoDIN to include rerouting, restoring or isolating.

- EX. CPT operations conducted on key terrain in cyberspace for mission-critical assets in response to indications of malicious cyberspace activity.

Defensive Cyberspace Operations - RA

- The form of DCO missions where actions are taken **external** to the defended network or portion of cyberspace without the permission of the owner of the affected system.
  - Normally in foreign cyberspace
  - May include actions that rise to the level of use of force
  - Require properly coordinated orders

Offensive Cyber Operations (OCO)

- **Purpose/Intent:** Execute effects in and through foreign cyberspace through actions taken in support of CCDR or National objectives. Actions may result in use of force with physical damage or destruction of enemy systems/terrain.
- **Goals:** Exclusively target adversary cyberspace functions or create first-order effects impacting the physical domains (Kinetic vs Non-Kinetic)
  - Deny, Degrade, Disrupt, Destroy enemy terrain

Requires coordination and careful consideration of scope, ROE, and measurable objectives

Cyber Mission Forces (CMF)

- Cyber mission forces consist of 133 teams and 6,200 prsnl
  - Army provides 41/133
  - Navy provides 40/133
  - Air Force provides 39/133
  - Marine corps provides 13/133

Cyber Mission Forces (CMF)

- Of those 133 teams:
  - 13 are National Mission Teams (NMTs) that **defend the nation.**
  - 68 are Cyber Protection Teams (CPTs) that work to **defend DoD networks.**
  - 27 are Combat Mission Teams (CMTs) that **provide support** to **CCMDs** and **generate effects** in support of operational plans and contingencies
  - 25 are **support teams** that provide analytic and planning support to NMTs.

Cyber National Mission Force (CNMF)

- Cyber National Mission Force operate to **defeat significant cyberspace threats** to the DoDIN and the Nation.
- **National Mission Teams (NMTs):**
  - Aligned to a malicious cyber actor, meaning they are often in grey and red space.
- **National Support Teams (NSTs):**
  - Linguists and analysts who support mission teams
  - Serve in an intelligence role, providing analytical and planning support to the national mission and combat mission teams

Cyber Protection Forces (CPF)

- Cyber Protection Forces provide **internal protection** of the DoDIN or other blue cyberspace.
- Consists of 68 Cyber Protection Teams (CPTs) that organize, train and equip to defend assigned cyberspace in coordination with and in support of the Cyber National Mission Force.

Cyber Combat Mission Force (CCMF)

- Cyber Combat Mission Forces **support the missions, plans, and priorities** of the **geographic** and **functional CCDRs.**
  - Consist of Combat Mission Teams (CMTs) & associated Combat Support Teams (CSTs)
  - Provide **offensive cyber operations** to achieve or directly support Combatant Commander objectives.
  - Aligned toward Combatant Commander's campaign objectives but are no longer under the operational control of the Combatant Commanders.

Cyberspace Operations (OCO vs DCO)

- All actions in cyberspace that are not cyberspace-enabled activities are taken as part of three cyberspace missions:
  - Offensive Cyber Operations (OCO)
  - Defensive Cyber Operations (DCO)
  - DoDIN Operations (DoDIN)
- Authorized by military order (CTO, CCO, MTO etc)
- Cyber Operations require integration and synchronization of all three.

Types of Orders

OPORD/TASKORD	Direct Strategic / Operational Plan
FRAGO	Incremental Operations / Supplemental Order
CTO	Operational Orders issued by AFCYBER
CCO	Used to build/shape portions of cyberspace
MTO	Routine tasks that enhance network security
TCNO	Orders issued to direct **immediate** patching
SPINS	Amplifying instructions
NOTAM	FYI/FYSA, no specific actions to be taken

Types of Orders

- USSTRATCOM/USCYBERCOM issues orders via various formats that include but are not limited to **Operation Orders (OPORDs)** and **Tasking Orders (TASKORDs)**.
  - Orders received from USCYBERCOM ***(Combatant Command)*** will be relayed promptly, where applicable, through AFCYBER/CC or from his/her delegated representative to the 616 Operations Center to the tasked units.
  - The AFCYBER/CC through the 616 OC, may add AF-specific tasks to an OPORD; however, the original OPORD must remain intact.

Types of Orders

- **Operation Orders (OPORDs) / Tasking Orders (TASKORDs)**
  - Disseminated for direct implementation of an operational and strategic level plan.
  - Issued for the purpose coordinated execution of an operation.
  - Published and distributed by USCYBERCOM.

- **Fragmentary Order (FRAGO)**
  - Supplemental documents that provide additional instructions for incremental operations.
  - Like an addendum to an already published order/document.

Types of Orders

- **Cyber Tasking Order (CTO)**
  - Operational orders issued to perform specific actions at specific time frames in support of AF and Joint requirements.
  - Generally derived from USCYBERCOM and issued by AFCYBER via the 616 Operations Center.

- **Cyberspace Control Order (CCO)**
  - Used to build/shape the portion of cyberspace to be employed in support of a CCMD operation or in response to adversary actions.
  - Documents permanent modifications, updates and retrofits.

Types of Orders

- **Maintenance Tasking Order (MTO)**
  - **Routine tasks/updates** that enhance network security with a medium to low risk associated with the task.
  - Typically reach the lower echelons of the Air Force to ensure compliance is met (EX. Patching)

Types of Orders

- **Time Compliance Network Order (TCNO)**
  - Orders issued to direct the **immediate patching** of information systems to mitigate or eliminate exploitation vulnerabilities. These orders have a significant implication if not accomplished in a timely manner.
  - Prepared by AFCERT (33 COS)
  - CSCS units ensure compliance across the Air Force

Types of Orders

- **Special Instructions (SPINS)**
  - Provide amplifying instructions for planning, execution, and assessment of Air Force CTOs and CCOs.

- **C4 Notice To All Airmen (NOTAM)**
  - Can be issued at any level
  - Used to disseminate network information that does not direct specific action to be taken or compliance to be tracked.
  - Provides SA for matters not requiring acknowledgement

Types of Orders

OPORD/TASKORD	Direct Strategic / Operational Plan
FRAGO	Incremental Operations / Supplemental Order
CTO	Operational Orders issued by AFCYBER
CCO	Used to build/shape portions of cyberspace
MTO	Routine tasks that enhance network security
TCNO	Orders issued to direct **immediate** patching
SPINS	Amplifying instructions
NOTAM	FYI/FYSA, no specific actions to be taken

Cyber Security Controls

- **National Institute of Standards and Technology (NIST)** is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.
  - Established by the U.S. Congress in 1901.
  - The NIST publishes controls for systems and organizations that can be implemented within any organization or system that processes, stores, or transmits information.
  - The use of these controls is mandatory for federal information systems in accordance with the Office of Management and Budget (OMB).

Cyber Security Controls

- The NIST developed a broad list of categories of controls, below is a list of that usually apply specifically to system authorization. These categories list how to manage the risk depending on the system.

- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition

Cyber Security Controls

- **How does this apply to us in Cyber?**
  - DISA has selected the controls that apply to various pieces of hardware and software to meet baseline security requirements for our network.
  - Technical guidance on how to configure hardware or software are called the **Security Requirements Guide (SRGs)** and **Security Technical Implementation Guide (STIGs)**.
  - Compliance with these guides are **mandatory** because the DoD is required to manage their risk.

  - ***Ex.*** *Amn Snuffy wants to add a Cisco 2960 switch to the base network. DISA has already determined what is required before adding it. S/he would refer to the STIG in order to implement.*

STIG/SRG

- **Security Requirements Guide (SRG)**: General purpose guides for types of hardware or software. Is a minimum baseline guide for a broad range of equipment when adding to the network.
- **Security Technical Implementation Guide (STIG)**: Vendor specific guides that specifically detail how to configure hardware or software when adding to the network.
  - **No hardware or software may be added to the network unless approved in a Risk Management Framework Package.**
- Both SRG & STIGs are provided by DISA.

Information Assurance Vulnerability Management (IAVM)

- **Information Assurance Vulnerability Management (IAVM):** A web-based application that uses control mechanisms to mitigate software vulnerabilities that would otherwise jeopardize a system.
  - USCYBERCOM analyzes each vulnerability to determine if it's necessary or beneficial to the DoD to release as an Alert.
  - Alerts and Bulletins are published on https://iavm.csd.disa.mil/
  - Implementation of IAVA policy helps ensure DoD Components are taking appropriate mitigation actions against vulnerabilities to avoid serious compromises to their information systems.

IAVM Objectives (CJCSM 6520.02)

- Prevent adversary exploitation of disclosed vulnerabilities
- Identify and analyze disclosed vulnerabilities
- Prioritize remediation
- Provide a timeline to acknowledge
- Provide metrics to leadership

IAVA/IAVB

- **Information Assurance Vulnerability Alert (IAVA):** Addresses recently disclosed vulnerabilities that indicate **severe risk** to DoD Information Systems and **is the basis for TCNOs.**
- **Information Assurance Vulnerability Bulletin (IAVB):** Addresses recently disclosed vulnerabilities that **do not currently pose** an **immediate risk** but are significant enough that non-compliance could escalate risk and **is the basis for MTOs.**

Plan of Action & Milestones

- What happens when you cannot meet the deadline to a CTO or MTO?
  - You submit a **Plan of Action & Milestone (POA&M)**.
  - Submitted through the MAJCOM Communications Coordination Center(MCCC)
  - POA&M is a document that includes mitigation factors, and fix date to what ever order you cannot meet.