



# DISA Strategic Pitch Lionfish Cyber Security

Introducing the **Lionfish Cyber SHIELD Platform**

 Disabled Veteran Owned



## Contact Information

 Jeremy Miller, CEO

 +1 877-732-6772 Ext 701

 [Jeremy@LionfishCyberSecurity.com](mailto:Jeremy@LionfishCyberSecurity.com)

# Presentation Agenda



## Organization Overview

Introduction to Lionfish Cyber Security and our mission

5 min



## Capability Overview

The Lionfish Cyber SHIELD Platform and our "develop locally, select nationally" approach

20-25 min



## Live Demonstration

Showcase of the Cyber SHIELD Platform in action

15-20 min



## Questions & Answers

Open discussion and addressing your questions

10-15 min

# Organization Overview

## Lionfish Cyber Security

 **Disabled Veteran Owned**

 **Cyber Defense Specialists**

 **University Partnerships**

Lionfish Cyber Security is dedicated to securing America's digital infrastructure through innovative approaches that combine workforce development with practical cybersecurity implementation across the USA for Governmental entities, critical infrastructure and small business.

### Leadership



**Jeremy Miller**  
Chief Executive Officer

### Contact Information

 +1 877-732-6772 Ext 701

 [Jeremy@LionfishCyberSecurity.com](mailto:Jeremy@LionfishCyberSecurity.com)

## Our Mission

To address critical cybersecurity vulnerabilities across America while developing the next generation of cyber defenders through practical, hands-on experience.

### Core Capabilities



#### Talent Development

Building the cybersecurity workforce through university partnerships



#### Cyber Defense Implementation

Real-world security for local governments and critical infrastructure



#### National Security Impact

Creating a pipeline of mission-ready professionals for DISA

# Lionfish Cyber SHIELD Platform

## What is Cyber SHIELD?

An integrated cybersecurity solution powering our nationwide "develop locally, select nationally" talent development ecosystem.

### Our Approach:

Through local colleges, university and tech school partnerships, we train students as Cyber Sentinels who implement real-world cybersecurity compliance for local communities.



Immediate Security  
Improvements



Talent Pipeline  
for DISA

## Platform Components



### Workforce Development

Training students through practical experience with real-world security challenges



### Governance & Compliance

Frameworks and tools to implement security standards across organizations



### Risk Management

Assessment and mitigation strategies for cybersecurity threats



### Analytics Tools

Data-driven insights to identify security gaps and optimize defenses

**Transforming cybersecurity education from theoretical to practical—creating mission-ready professionals for DISA**

# The National Security Crisis

## What Are We Trying To Do?

### **Urgent National Vulnerability**

Thousands of vulnerable local governments and critical infrastructure entities across America have been infiltrated by nation-state actors who have already "prepped the battlefield" for potential cyberattacks.

### **Key Vulnerabilities:**

- No viable defense plans for these entities
- Critical infrastructure exposed to coordinated attacks
- Existing adversary footholds remain unaddressed

### **Our Holistic Approach:**

Leveraging technology, we focus on people first—organizing, training, equipping, and deploying them to address our nation's most vulnerable points in cybersecurity.

## Our Solution:

### Scalable "Cyber Cavalry"

Mobilize a nationwide network of trained defenders through university partnerships



#### **Immediate Security Implementation**

Harden vulnerable targets



#### **Adversary Disruption**

Identify and remove existing footholds



#### **Talent Pipeline Development**

Train cleared professionals for DISA

# Current Approach: The Security Gap

## How Is It Done Today?

### Today's Approach Is Failing

Current cybersecurity efforts are fragmented and reactive, with no coordinated national strategy to secure vulnerable points.

### Key Failures:

#### **CRITICAL** Workforce Gap

 DISA struggles with workforce challenges outlined in the WF2025 Implementation Plan

#### **HIGH RISK** Vulnerable Infrastructure

 Thousands of local governments and critical infrastructure entities sit vulnerable and compromised

#### **URGENT** No Coordinated Response

 Entities lack resources, expertise and personnel to defend themselves

## The Reality of Our National Cyber Landscape



*"If we focus solely on the technology required to do this and forget about the people who operate it, we will not only become stagnant, but we will also be outpaced."*

**- Lt. Gen. Skinner, WF2025 Plan**

 **We're leaving the digital keys to our nation in the hands of our adversaries**



# Our Innovative Approach

## What's New in Our Approach?

### The National Cyber Defense Corps

Mobilizing a scalable solution through our university-based Cyber Sentinel program—the only approach capable of addressing the massive scope of this crisis.



Immediate Threat Response



Scaling Defense Through Education



Building a Cleared Talent Pipeline



National Security Grid Development

### “ The Special Forces Principle

*"The first rule in Special Operations: **people are more important than equipment or technology**. We must cultivate the people—organize, train, equip and deploy them today in a scalable model."*

## Why Will This Approach Succeed?

### People-Centered Solution

- ✓ Focusing on human capital, not just technology

### Matches Scale of Threat

- ✓ Proportional response to the nationwide crisis

### Dual-Purpose Approach

- ✓ Addresses immediate vulnerabilities and workforce development

### Real-World Experience

- ✓ Practical training against actual advanced threats

### Ground-Up Security

- ✓ Strengthening the entire national infrastructure

### Self-Reinforcing Ecosystem

- ✓ Where education directly enhances security

# Who Cares? The Stakeholders

The stakes could not be higher, with multiple critical stakeholders deeply invested in this solution:



## National Security Leadership

Facing the reality that adversaries have already established footholds across thousands of vulnerable systems nationwide.



## DISA and DoD Leadership

Recognizing that their mission is compromised if the broader ecosystem of local governments and critical infrastructure remains vulnerable.



## Local Governments

Currently sitting exposed to advanced persistent threats without viable defense options.



## Critical Infrastructure

Responsible for systems that support national function but lacking adequate cybersecurity resources.



## Homeland Security

Concerned about cascading failures across interconnected infrastructure systems.



## The American Public

Whose safety, privacy, and essential services are at risk from coordinated cyberattacks.

“If we focus solely on the technology required to do this and forget about the people who operate it, we will not only become stagnant, but we will also be outpaced.”

- Lt. Gen. Skinner, WF2025 Plan

**This crisis requires both technology and human capital solutions—exactly what our approach provides.**



# | If We're Successful: The Impact

Success creates a fundamental shift in our national cybersecurity posture:



## Adversary Disruption

Identify and remove existing nation-state footholds in thousands of local systems



## Infrastructure Protection

Essential services become resilient against coordinated attacks



## National Security Grid

Create an interconnected network of secured entities with shared awareness



## Workforce Transformation

DISA accesses professionals who've confronted advanced threats in real environments



## Defense in Depth

Shift from thin federal defense to multi-layered defense starting at local level



## Strategic Reversal

Turn our greatest vulnerability into a strategic asset through distributed security



## Human Capital

Develop cyber defenders who understand operational security implementation



## Sustainment Model

Create an ongoing ecosystem that continuously strengthens security while developing talent






## Beyond Workforce Development



This isn't just about talent acquisition—it's about **preventing potentially catastrophic coordinated cyberattacks** against our nation's fundamental infrastructure by putting the right people in the right places with the right training.

# Risks & Payoffs

## Risks

-  Discovery of more extensive nation-state compromise than anticipated
-  Potential escalation of adversary activities when their footholds are threatened
-  Coordination challenges across thousands of diverse entities
-  Security considerations when engaging students with compromised systems
-  Initial funding may be insufficient for the full scope of the national crisis

## Payoffs

-  Disruption of adversary pre-positioning across thousands of American systems
-  Creation of the first truly national cybersecurity defense capability
-  Development of professionals with real-world experience countering nation-state actors
-  Transformation of our cybersecurity posture from reactive to proactive
-  Protection of essential services and critical infrastructure from coordinated attacks
-  Establishment of a sustainable model that continuously strengthens security
-  Positioning DISA at the forefront of innovative national defense approaches
-  Building a human-centered security ecosystem that doesn't just rely on technology

# Program Costs & Investment

## \$10M

Initial funding requirement for a 2-year pilot

To demonstrate the model's effectiveness and build foundation for national expansion



**1,000+ Students**

Trained as Cyber Sentinels across 20+ universities nationwide



**200+ Entities**

Secured nationwide, disrupting existing adversary footholds



**200+ Candidates**

Identified for DISA's workforce pipeline with relevant experience

Projected 2-Year Impact of \$10M Investment



## The Cost of Inaction



Leaving thousands of critical systems vulnerable to coordinated attacks could cost our nation incalculably more in **economic damage, critical service disruption, and potential loss of life.**

# Implementation Timeline

Our implementation creates both immediate security improvements and long-term defense capability over a 24-month period:



## Phase 1

### Months 1-3

Program design  
Initial university partnerships  
5 strategic regions



## Phase 2

### Months 4-6

Curriculum development  
Faculty training  
Student recruitment



## Phase 3

### Months 7-12

First cohorts begin implementing cybersecurity measures  
Identifying existing adversary footholds  
Disrupting nation-state access



## Phase 4

### Months 13-18

Security improvements at 100+ entities  
Initial clearance processes  
DISA candidate identification



## Phase 5

### Months 19-24

Security improvements at 200+ entities  
First fully-prepared candidates ready  
DISA position placement

## Urgency of Action



This aggressive timeline recognizes the urgency of the threat—our adversaries have already spent years preparing this battlefield, and every day of inaction increases our national vulnerability. By focusing on **people first**—organizing, training, equipping, and deploying them with purpose—we can move much faster than traditional technology-centered approaches.

# Success Metrics

The midterm and final "exams" to check for program success:










## Midterm "Exams"

-  **10+ universities** with Cyber Sentinel teams within 6 months
-  **100+ local entities** with cybersecurity improvements in first year
-  Remediation of adversary footholds in **50+ critical systems**
-  Identification of **50+ DISA candidates** with clearance initiated
-  Establishment of **secure threat intelligence** sharing network
-  Development of **rapid response protocol** for critical vulnerabilities



## Final "Exams"

-  **200+ entities** with improved cybersecurity posture and monitoring
-  **Documented disruption** of adversary pre-positioning across sectors
-  **200+ qualified candidates** in DISA's workforce pipeline
-  Placement of **50+ program graduates** into DISA positions
-  Establishment of a **self-sustaining model** for ongoing security
-  Creation of a **national threat intelligence network**
-  Development of a **scalable model** ready for national expansion

# Lionfish Cyber SHIELD Platform Demo

## What You'll See Today

A hands-on demonstration of how our platform transforms cybersecurity education into real-world security implementation while building DISA's talent pipeline.



In the next **15-20 minutes**, we'll demonstrate how the Lionfish Cyber SHIELD Platform enables us to:



### Train Cyber Sentinels

See our university training portal where students learn to identify and mitigate real-world cybersecurity threats using our integrated learning modules.



### Implement Security Controls

Watch a live demonstration of our compliance framework implementation for a local government entity, showing before and after security postures.



### Identify & Disrupt Threats

Experience our threat detection capability that identifies and neutralizes existing nation-state adversary footholds within vulnerable systems.



### Talent Pipeline Analytics

Preview our performance analytics dashboard that identifies top performers for DISA's workforce pipeline based on real-world implementation success.



## Key Demonstration Objective

To show how our model transforms the national security crisis into an opportunity—building a nationwide cyber defense capability while developing mission-ready professionals for DISA.



# Cyber Sentinel Training Program

## Developing Mission-Ready Professionals

### University Recruitment

Students recruited from cybersecurity programs across partner universities nationwide.

### Specialized Training

Intensive training on real-world security implementation and advanced threat detection.

### Field Deployment

Supervised implementation of security controls at local government and critical infrastructure entities.

### Performance Tracking

Continuous assessment identifies top performers for DISA's workforce pipeline.

## Demo Highlights

Key platform features you'll see during the demonstration:



### Training Portal

Interactive learning modules with real-world scenarios and hands-on labs.



### Assessment Engine

Automated skills verification and competency tracking across security domains.



### Field Operations

Implementation tracking and reporting for security measures across entities.



### Talent Analytics

Identifying top performers based on implementation success and security impact.



## Program Results

Real-world experience against actual threats, creating mission-ready professionals with practical skills.

# Security Implementation & Threat Disruption



## Security Implementation

### ✓ Compliance Framework Deployment

Automated implementation of NIST and CMMC controls across local entities

### ✓ Continuous Monitoring

24/7 security posture monitoring with real-time alerts

### ✓ Vulnerability Management

Identification and remediation of system vulnerabilities

### 📈 Implementation Results

- 85% reduction in critical vulnerabilities
- 100+ security controls implemented per entity
- Full NIST CSF alignment within 90 days



## Nation-State Threat Disruption

### Advanced Threat Detection

Identifying sophisticated nation-state actor activities across local systems



#### Persistent Access Mechanisms

Disrupting established backdoors and footholds



#### Data Exfiltration Channels

Detecting and closing unauthorized data channels



#### Attack Preparation Indicators

Identifying pre-positioned attack components



### Demo Highlight

Live demonstration of threat detection and response for a compromised municipal water system

# Talent Pipeline: From Cyber Sentinels to DISA Workforce



## University Recruitment

Nationwide talent selection from partner universities



## Cyber Sentinel Training

Real-world security implementation experience



## Performance Assessment

Identification of top performers for DISA pipeline



## DISA Workforce Entry

Cleared professionals with real-world experience

## Talent Analytics Platform Demo

Our platform provides comprehensive talent assessment and tracking:



### Performance Metrics

Quantifiable scoring across technical skills and implementation success



### Competency Tracking

Domain-specific expertise identification and development



### Security Clearance

Integrated clearance tracking and processing

## 🎯 Key Program Metrics

- 200+ qualified candidates in DISA pipeline annually
- 85% retention rate for placed candidates
- 3x faster time-to-productivity vs traditional hires

## 💬 Candidate Testimonial

*"The Cyber Sentinel program gave me hands-on experience against actual nation-state threats that no classroom could provide. I joined DISA with practical skills already applied in the field."*

— Alex Chen, Former Cyber Sentinel, Current DISA Analyst

# Leadership Forged in Empowerment & Innovation



**Jeremy Miller**

CEO - Green Beret Veteran, Serial Entrepreneur

[Jeremy Miller](#) | [LinkedIn](#)



**Dr. Shadi Jawhar**

CTO/Tech Lead

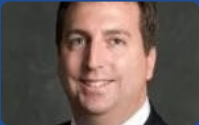
[Shadi Jawhar](#) | [LinkedIn](#)



**Marlon Williams**

CFO

[Marlon Williams](#) | [LinkedIn](#)



**Matt Pitchford**

CMO

[Matt Pitchford](#) | [LinkedIn](#)



**Mike Kolodkin**

Sales Leadership

[Mike Kolodkin](#) | [LinkedIn](#)



**Ryan Bardes**

Training & Student Programs Lead

[Ryan J. Bardes](#) | [LinkedIn](#)



**Dr. Diane Janosek**

Strategic Cyber Engagement

[Diane M. Janosek, PhD, JD](#) | [LinkedIn](#)



**Dawn Yankeelov**

Marketing and Grants

[Dawn Yankeelov](#) | [LinkedIn](#)



**Tony Selzo**

Strategic Business Development

[Tony Scelzo](#) | [LinkedIn](#)

A balanced team combining elite military strategic thinking, deep cybersecurity and GRC knowledge, educational expertise, and proven business scaling experience – all committed to the mission.



Accredited Training Provider  
(ATP)



Teaching: Certified CMMC Professional  
(CCP)



Teaching: Certified CMMC Assessor  
(CCA)



By: Certified CMMC Provisional  
Instructor (PI)



Service-Disabled Veteran  
Special Forces



"Together, we can secure the digital future—one community at a time."

# Questions & Answers



## 10-15 Minutes Allocated

We welcome your questions about Lionfish Cyber Security and our SHIELD Platform

### Suggested Discussion Topics

#### Implementation Strategy

Questions about nationwide deployment and scaling capabilities

#### Technical Capabilities

Detailed inquiries about the SHIELD Platform's security features

#### Talent Development

Questions about how we identify and prepare candidates for DISA

#### Partnership Opportunities

Exploring collaboration models between Lionfish and DISA

### Quick Reference Points

- ✓ Disabled Veteran Owned Small Business
- ✓ \$10M Initial Investment for 2-Year Pilot
- ✓ Nationwide University Partnership Network
- ✓ 200+ Local Entities Secured in Pilot
- ✓ 200+ DISA Workforce Candidates Identified
- ✓ Proven Nation-State Threat Disruption



**Jeremy Miller - CEO**

 +1 877-732-6772 Ext 701 |  [Jeremy@LionfishCyberSecurity.com](mailto:Jeremy@LionfishCyberSecurity.com)



# Moving Forward Together: Securing Our Nation

*"The Lionfish Cyber SHIELD Platform transforms our greatest vulnerability into our greatest strength—creating a nationwide defense while developing mission-ready professionals for DISA."*



## Immediate Threat Disruption

Identify and remove existing nation-state footholds across critical infrastructure



## DISA Workforce Pipeline

200+ qualified, experienced candidates ready to strengthen your mission



## National Security Grid

Transform vulnerable points into an interconnected defensive network

## Strategic Advantages

- ✓ People-centered solution with proven Special Operations principles
- ✓ Addresses both immediate threats and long-term workforce needs
- ✓ Nationwide scale matching the scope of the threat
- ✓ Self-reinforcing ecosystem of security and education

## Partner With Lionfish Cyber Security

Invest in our nation's cybersecurity future with the Lionfish Cyber SHIELD Platform

 **Initial Investment: \$10M for 2-Year Pilot**



**Jeremy Miller - CEO**

 +1 877-732-6772 Ext 701 |  [Jeremy@LionfishCyberSecurity.com](mailto:Jeremy@LionfishCyberSecurity.com)