Senior Management Official Roundtable

Jeff Afflerbach
President & CEO
Mantis Security Corporation

Christopher Rodgers
CEO
SYNAPP, Inc

Mantis Security Corporation was founded in 2015 by an ISSO and an Architect… now is a leading cybersecurity firm that primarily provides trusted programmatic, strategic, and technical services to the Intelligence Community. Our clients and partners rely on our depth of technical expertise to support their mission objectives. The team provides C-level strategy and program support to a variety of large agencies, specialized missions, and commercial industries.

We foundationally began with Systems Architecture and Information Assurance to ensure that cybersecurity evolves throughout the system lifecycle. Our experts advise decision makers on emerging threats and technologies; we initiate and lead agency-wide initiatives. Integrity and quality of service is evident across our team of trusted advisors in all aspects of IT Security Automation, Cyber-AI Innovation, Zero Trust Strategy, Security Architecture and Engineering, Risk Management Framework (RMF), and technical Leadership.

Jeff Afflerbach

CISM, CISSP

Leading Mantis Security with over 25 years of experience in the Information Technology and Security fields. Jeff started as a US Marine in Counter-Intelligence & HUMINT as an Arabic Linguist; he also focused as an IAVM/Data Security Classified Spillage Specialist/CERT at MCNOSC, additionally filling the billet of IT Training Chief and Assistant PM.

Formerly of DSD Labs, President of AGI, and Security Assessor for numerous FedCiv, DoD, and IC agencies, in 2015, Jeff founded Mantis Security Corporation where he currently serves as the President & CEO. He also serves as the organization's Facility Security Officer.

Jeff loves motorsports and spends most weekends chasing lap times at Sebring and other east coast racetracks.

www.mantissecurity.com

SYNAPP

DELIVERING NEXT-GEN CYBER SOLUTIONS

SYNAPP, a Service-Disabled Veteran-Owned Small Business (SDVOSB), represents a unique convergence of technology and biology, encapsulating the essence of connectivity and security in the digital realm, much like a synapse does in the human brain. At its core, it embodies the process of initiating and authenticating connections, symbolized by the SYN/SYN-ACK/ACK handshake in networking, while also functioning as an application designed to perform critical operations.

This innovative approach allows SYNAPP to serve as a digital synapse, bridging gaps between disparate pieces of information, thus facilitating seamless communication and integration. By mimicking the biological function of synapses, which are crucial for neuronal communication and information processing, SYNAPP aims to enhance the security and efficiency of digital ecosystems.

Christopher Rodgers

Over 20 years of experience as a contractor and USAF Cyber Airman, Chris has led teams in securing mission-critical systems across diverse domains, including GPS/PNT, MILSATCOM, and SBIRS. His expertise spans Risk Management Framework (RMF) compliance, DISA STIG implementation, penetration testing, and automation of cybersecurity processes using tools such as Ansible, Terraform, and SIEM monitoring. Under his leadership, SYNAPP has earned a reputation for delivering innovative, reliable, and security-focused solutions that enhance national defense operations, while fostering strong partnerships with government and industry stakeholders

www.synapp.com

Topic #1

The SMO has ultimate authority over the facility's operations and the authority to direct actions necessary for the safeguarding of classified information in the facility.

What do you feel are your biggest challenges for meeting this requirement, considering that the SMO usually wears multiple hats and often has a primary focus of growing the organization?

Topic #2

When considering things like common approach vectors (e.g., known Methods of Contact/Methods of Operation), do you personally seek out additional information or do you primarily lean on your FSO to provide you with information?

If you do personally seek out information, are there any resources or sites that you have found to be helpful?

Topic #3

32 CFR 117.7(b)(2)(iv) requires the SMO to make decisions based on classified threat reporting and their thorough knowledge, understanding, and appreciation of the threat information and the potential impacts caused by a loss of classified information.

As the SMO, what kind of considerations do you take into account when making such decisions? How often do you find that threat reporting ends up directly impacting your business decisions?

Topic #4

How do you include your FSO, or security staff, in business decisions that can impact the organization’s security program?

Topic #5

How do you balance the requirements for maintaining a sufficient number of security staff with the need to keep overhead costs within a manageable level?

Topic #6

Do you actively take part in the organization’s security program (e.g., interacting with managers on security requirements) and are there any considerations that you find are particularly helpful with ensuring a proper security culture within the organization?

Topic #7

Could you identify something that you know now as an SMO that you wished you'd known when you first started in the position?

Any advice that you feel is particularly relevant for new SMOs?

Topic #8

Are there any other best practices or actions that you have found increase your company's overall security performance or better prepare you as the SMO for meeting NISPOM compliance?

www.mantissecurity.com

Questions?

www.synapp.com