



# Industry Insights - Cybersecurity for Additive Manufacturing

Additive Manufacturing for Reactor Materials & Components  
November 28, 2017

Scott Zimmerman, CISSP-ISSEP  
Chief Information Security Officer /  
Principal Cybersecurity Engineer  
[email: sdz@ctc.com](mailto:sdz@ctc.com)  
twitter: @zimmy266

# Agenda

- Introduction
- Threat Update - FUD
- Cybersecurity for Direct Digital Manufacturing (DDM)
- Cybersecurity Regulations
- Supply chain
- Recommendation

# CTC - Leading Innovation through Engineering, Technology and Services

## **Concurrent Technologies Corporation (CTC)**

is an independent, nonprofit, applied scientific research and development professional services organization.

**Enterprise Ventures Corporation (EVC)** is CTC's technology commercialization arm and is organized as a wholly owned for-profit affiliate of CTC.

CTC and EVC provide full lifecycle support services to clients, from innovative concepts through production and deployment.

30

YEARS OF  
INNOVATION

600

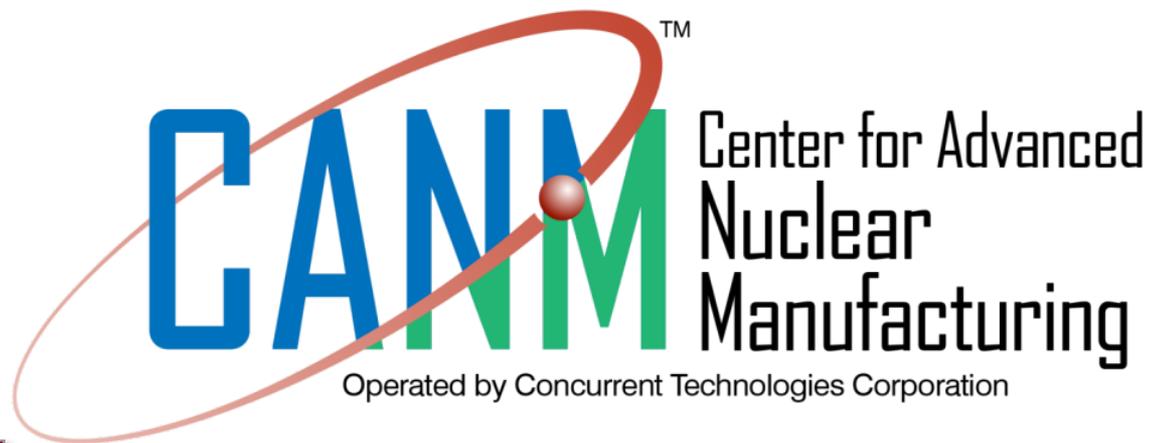
EMPLOYEES

25

LOCATIONS

# Center for Advanced Nuclear Manufacturing

- With the advent of the next generation of SMRs and AR's there is a clear need for advanced manufacturing technologies to support the efficient fabrication of complex modular systems
- In 2017 CTC made the decision in 2017 to establish the Center for Advanced Nuclear Manufacturing (CANM) with support from the US Nuclear Infrastructures Council's
- Leverages CTC's experience in operation of the Navy Metalworking Center (NMC) helps to facilitate an efficient start-up and operation of the Center



# Cyber Threat Update

# Threat update

- Verizon Breach Report (November 10, 2017)
  - 75% of breaches were from external actors, 25% involved internal actors
  - 62% featured hacking, 51% included malware, 81% were **stolen or weak passwords**
  - 66% of malware **installed via email**
  - 73% were financially motivated with **21% being espionage**
  - 61% of the victims were businesses **under 1,000 employees**
- Manufacturing specifics results
  - 90% of data stolen during a breach were considered “**secrets**” by the owner
  - **Strategic gains** were the number one motive
  - The majority were conducted by **state-affiliated sponsored actors**
  - Internal espionage was present as well

# When were you compromised?



**DARKReading** | Join us live at **INSECURITY** | A Dark Reading Conference

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

ANALYTICS ATTACKS/BREACHES APP SEC CAREERS & PEOPLE CLOUD ENDPOINT IoT MOBILE OPERATIONS

ATTACKS/BREACHES

**FOX NEWS Tech**

Home Video Politics U.S. Opinion Business Entertainment Tech Science Health Travel Lifestyle

**HACKERS**

### Ransomware attack costs South Korean company \$1M, largest payment ever

Published June 21, 2017 · Fox News

Advertisement

Trending in Tech

- Wasn't ripe for video
- Robot dogs
- Removal of
- Additional
- claims

## 'Bad Rabbit' Ransomware Attacks Rock Russia, Ukraine - and Beyond



## 200 Million Hacked YAHOO! Accounts Up On SALE

**Yahoo 200M**

By [peace\\_of\\_mind](#) (100.0%) Level 1 (14)

0.0000 / BTC 3.0000

In Stock

Postage Option

Buy It Now

Escrow Yes, escrow by RealDeal is available.

Class Digital

Ships From Worldwide

## Another big malware attack ripples across the world

by Alanna Petroff and Selena Larson @CNNTech

June 28, 2017 2:14 PM ET

How to protect yourself from hackers

Hackers launched blistering ransomware attacks Tuesday against companies and agencies across the world, particularly targeting Ukrainian businesses.

Major global firms reported that they had been targeted, including British advertising agency WPP (WPPGY), Russian oil company Rosneft, and British energy giant EDF Energy.

Technologies Partners Company Resources



## "ride" Malware Causes City Alert

[metand Security](#) has issued a

**IRS**

Help | News | Language | **Charities & Nonprofits** | **Tax Pros**

File | Pay | Refunds | Credits & Deductions | Forms & Instructions

Home > News > [News Releases](#) > Dangerous W-2 Phishing Scam Evolving Targeting Schools Restaurants Hospitals Tribal Groups and Others

## Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others

# Why are we still failing?

- We have big budgets for security...
- We are focusing on the right things, I think...
- There is a shortage of talent but is that really the reason...
- Is the adversary that motivated or smarter...
- Are our workforce the issue...
- Do we not train enough or the right way...
- Is this just the new norm...



# Cybersecurity for DDM

# Cybersecurity: A Practical Perspective

Can you  
connect our  
new  
printer?



# Direct Digital Manufacturing

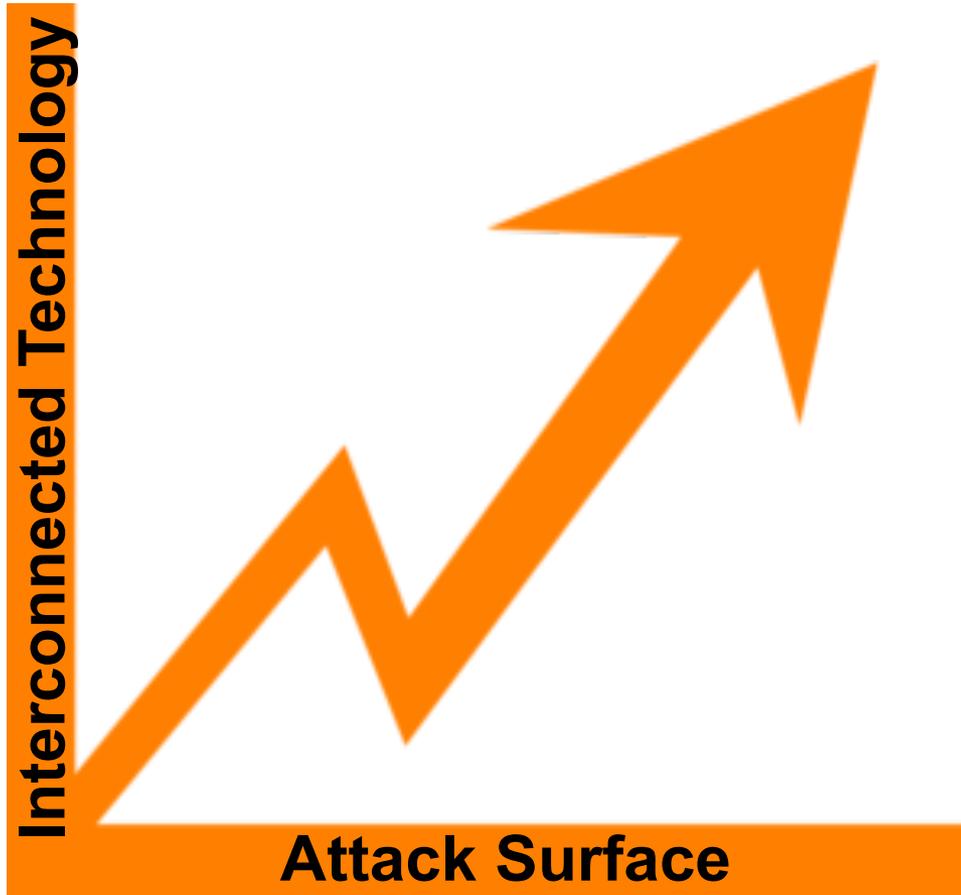
- *“The fabrication of components in a seamless manner from computer design to actual part in hand”- Brookings Institute*
- A disruptive technology with similar communication challenges as with Control Systems and IOT sensors
- Air gapped cybersecurity approach cutting the “Digital Thread”



# Industrial Control System Cyber Issues

- ICS-CERT 2016 Report ICS Findings
  - Boundary protection
  - Least functionally
  - Authenticator management
  - Identification and authentication 5. Least privilege
  - Allocation of resources

# Advanced Manufacturing Security Challenges



## RISK

- Loss or theft of intellectual property
- Compromised process and/or product integrity
- Productivity disruption
- Damage to reputation

# Additional Research

- CTC cyber risk assessment
- NIST Symposium on DDM
  - <https://www.nist.gov/publications/proceedings-cybersecurity-direct-digital-manufacturing-ddm-symposium>
- Textbook chapter
  - “Cybersecurity for Industry 4.0”
  - <http://www.springer.com/us/book/9783319506593>

## Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing Systems

Scott Zimmerman, CISSP-ISEP  
Concurrent Technologies Corporation  
Johnstown, PA USA  
zimmerms@ctc.com

Dom Glavach, CISSP  
Concurrent Technologies Corporation  
Johnstown, PA USA  
dg@ctc.com

*Abstract* – Applying meaningful and cybersecurity controls are ongoing an for the Direct Digital Manufacturing (DDM). These issues will be significant as the the mainstream manufacturing supply presentation will therefore address cy DDM, including insight into potential motivations, gained through direct ob discuss the details of a security assess Additive Manufacturing (AM) system prototyping and complex part produc industry. Protocols and associated rec incorporating security best practices c and subsequent operation will also be

*Keywords*—additive manufacturing, manufacturing, programmable logic con

### I. INTRODUCTION

Based on the expectation and potent the US and global manufacturing (AM) and other similarly disruptive significant impact on national sec National Defense University, “T technology has generated a hos considerations, which connect to bro developments...Additionally, the technologies in manufacturing will interaction between the national sec private sector, as businesses will be a and sophisticated components more i than before.” While supply chain i are numerous, cybersecurity remains

The Economist (April 2012) refers to create the third industrial revol disruption to manufacturing will digitization was to telecommuni photography and publishing. While incredible growth potential within

Springer Series in Advanced Manufacturing

Lane Thames  
Dirk Schaefer *Editors*

## Cybersecurity for Industry 4.0

Analysis for Design and Manufacturing

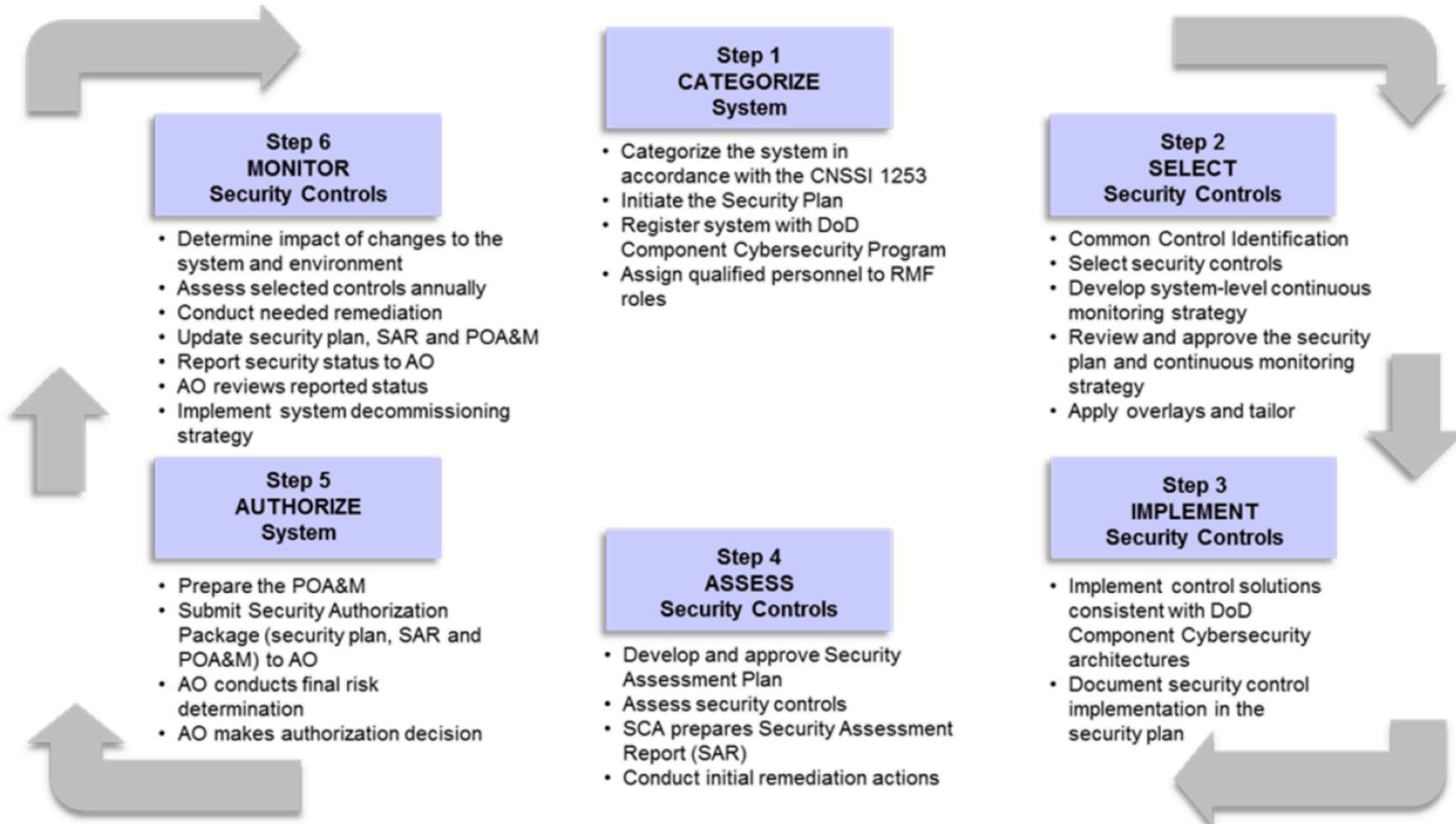
 Springer

# DoD Cybersecurity Requirements

# DoD Information Assurance Framework Evolution

- DoD Information Technology Security Certification and Accreditation Process (DITSCAP), mid 1990s
  - Standardized approach, did not take into account evolving threat landscape
- DoD information Assurance Certification and Accreditation Process (DIACAP), 2006
  - Recognized an acceptable operational risk level to support mission
- DoD Information Assurance Risk Management Framework (DoD RMF), 2013
  - Risk based approached to managing cybersecurity

# DoD Risk Management Framework

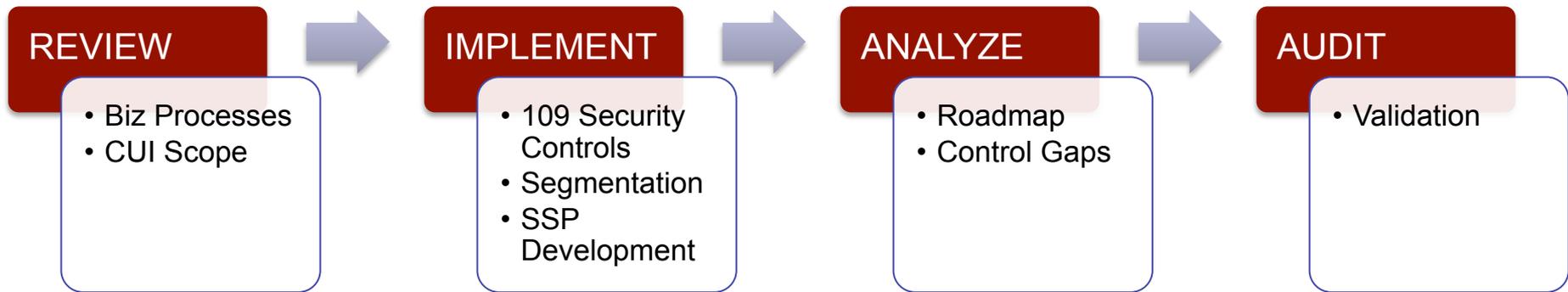


<https://aida.mitre.org/cyber-rmf/>

# USG/DoD Contractor Cyber Requirements

- **NIST** issued cyber safeguards (Special Publication 800-171) in June 2015 to protect CUI in non-federal information systems.
- **DoD** issued the “Network Penetration” DFARS in Aug. and Dec. 2015 and these were revised on Oct. 21, 2016.
- **Federal civilian agencies** issued a new FAR “Basic Safeguarding” clause, effective June 15, 2016, requiring all contractors to protect “Federal Contract Information” on “Information Systems.”
- **NARA** issued the Final Rule on “Controlled Unclassified Information” (CUI) on Sep. 14, 2016.
- A “**General FAR Rule**” is in development that will obligate all federal agencies to require cyber protection of CUI, per SP 800-171, in all contracts and agreements. Expect this Rule to be final in 2017.

# Path to NIST SP800-171 Compliance



# SMB Supply Chain Cybersecurity Issues

- Small suppliers/businesses have become a prime target for attackers and act as a stepping stone to primes
  - From janitorial services to software engineering-- with physical or virtual access to information systems, software code, or IP
- Small businesses are spending less on cyber security while large businesses are spending more
- Small businesses generally don't have formal cyber security awareness efforts for their employees

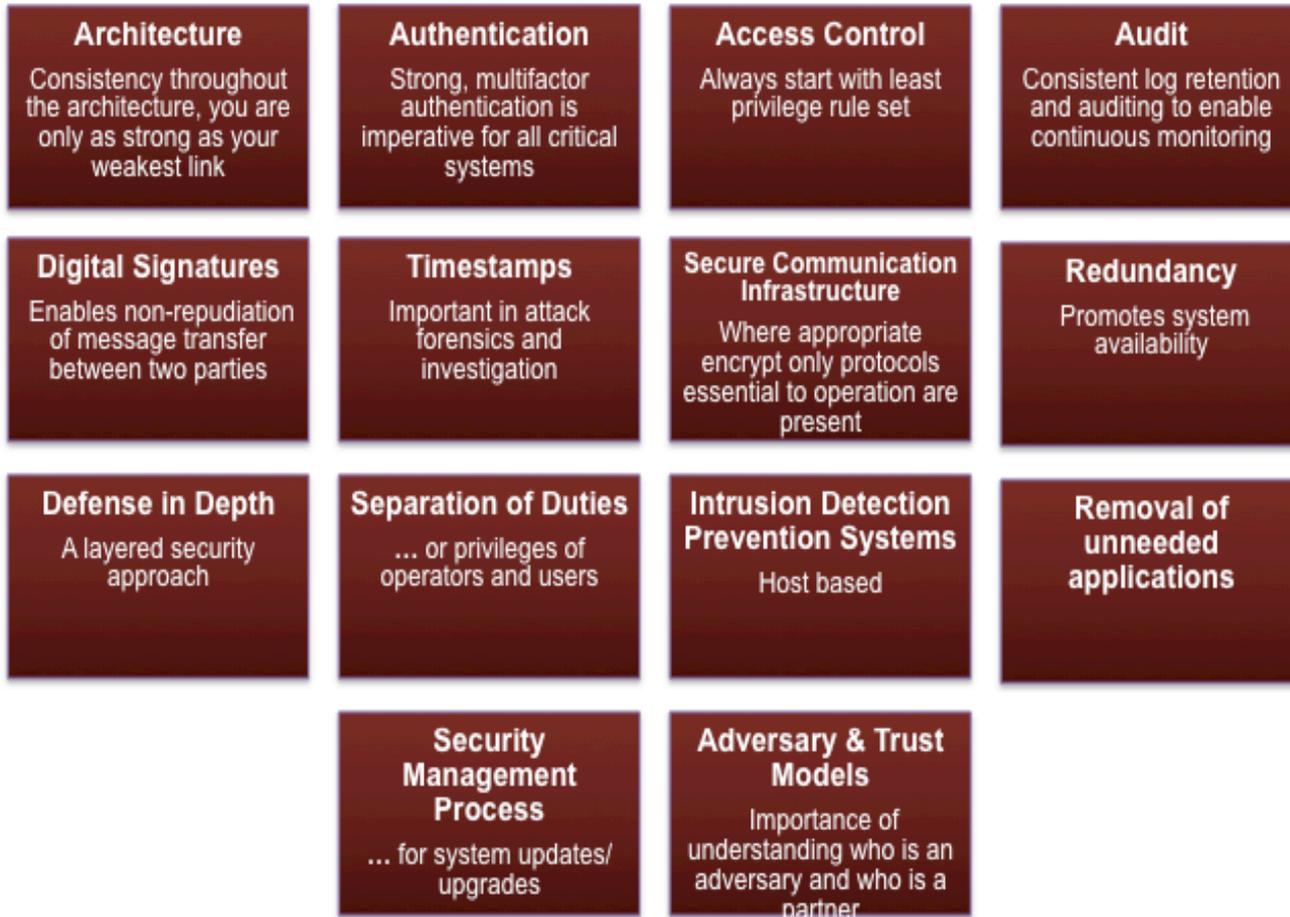
## Supply chains cyber risk ..



# Recommendations

- Learn lessons from past industry digitization
  - Telecom with the Internet of Things (IOT) to digital photography
- Now is the time to build cybersecurity into the process
  - Corporate leadership tends to be reactionary, we must get ahead of disruptive technology
  - Address cybersecurity concerns throughout the component lifecycle
  - Create active defense, don't wait to respond
  - Don't bolt it on at the end...

# Cybersecurity Recommendations



# QUESTIONS?

# Center for Advanced Nuclear Manufacturing

- With the advent of the next generation of SMRs and AR's there is a clear need for advanced manufacturing technologies to support the efficient fabrication of complex modular systems
- Two organizations have recently developed models for a manufacturing technology center for U.S. nuclear industry -
  - DOE NE vision for a nuclear advanced manufacturing technology center
  - USNIC's concept for a U.S. Virtual Advanced Manufacturing and Research Center (VNAMRC)
- Leveraging CTC's experience in operation of the Navy Metalworking Center (NMC) helps to facilitate an efficient start-up and operation of the Center -
  - Transferrable experience and capabilities
  - Extensive experience in managing project identification and development efforts
  - Experienced management and technical staff with "right mix" of skills.

# CANM Operation

- With USNIC's support, CTC made the decision in 2017 to establish the Center for Advanced Nuclear Manufacturing (CANM)
- CANM will utilize existing metalworking capabilities to establish a self-sustaining global resource to develop and deploy applied metalworking and manufacturing capabilities to advance SMR / AR design, fabrication and operation
  - Bring together the right mix of technologists, engineers and solution providers from industry and academia to develop and demonstrate cost effective and implementable technical solutions
  - Provide manufacturing and demonstration facilities to support the fabrication and testing of functional prototype systems
- CANM is initially being operated as an industry-funded organization
- DOE is working to establish an advanced manufacturing technology center with an industry cost-share requirement for awarded projects.