Increasing Access to NSA's Industrial Base: Cybersecurity and Mid-Tier Companies, and North American Industrial Classification System (NAICS)

Leslie Lewis

May 2017

Issues

- What role does the North American Industrial Classification System (NAICS) play in US government procurement?
- Do the current NAICS codes encompass the full spectrum of cybersecurity workforce requirements?
- Do the NAICS hinder NSA's access to IT and cybersecurity services and products
- What gaps exist and how might the NAICS be improved to expand NSA's access to its industrial base?
- How might NSA improve its access to mid-tier companies?

Insights

- NAICS was designed in the 1930s to assess health of industrial bases in Canada, US, and Mexico
- 1970s it evolved into US government procurement tool
- NAICS drive a lot of how the government buys its products and services
- NAICs are structured around generic categories for products and services
- NAICS limits access to the full spectrum of cybersecurity capabilities
- Data suggests that NSA is accessing small portion of cyber-qualified companies for products and services, as is all of the US government
- Numbers of mid-tier companies working in the government space is constricting, while the number of mid-tier cybersecurity commercial companies is growing

Insights

- Government access to mid-tier companies is essential to getting innovative technologies and a qualified and affordable contractor workforce
- Small companies are incentivized to grow and become mid-tiers; once a company becomes a mid-tier the companies encounter significant government dis-incentives because of how NAICs
- Many mid-tier and small companies are unaware of the importance of NAICS codes in doing business with the government
- Establishment of cybersecurity NAICS is feasible
- US government agencies have the authorities to conduct individual “prototype” acquisitions to get cybersecurity-unique skills and functions, and better access to mid-tier companies

North American Industry Classification System (NAICS)

- Consists of two major categories: Products and Services
- NAICS is used for majority of DoD and IC market research, surveys, RFIs and Requests for Proposals (RFPs)
- NAICS categories defined for small and large companies
- The US Industrial base is complex with many stratums especially in "mid-tier" arena; none of this complexity is reflected in the NAICs structure

NAICS, Cybersecurity, and Industrial Base

- **Cybersecurity does not align within one, two or three primary industries in NAICS**
- **The NAICS structures do not contain industry strata that represent business in the cybersecurity industry**
- **Seven NAICS categories <u>somewhat</u> align but are generic and must be "tweaked" to incorporate cyber capabilities**
  - 3341: Computer and electronic product manufacturing
  - 3342: Communications equipment manufacturing
  - 3364: Aerospace product and parts manufacturing
  - 5112: Software publishers
  - 5415: Computer systems design and related services
  - 5416: Management, scientific and technical consulting services
  - 5417: Scientific research and development services
- **Government tapping into very small percentage of the cyber industrial base; San Diego sampling showed:**
  - 7 percent of computer systems design and related service firms (NAICS: 5415) were cyber employers
  - 3 percent of management, scientific and technical consulting firms (NAICS: 5416)
  - Defense and aerospace were most important categories followed by
  - Technology/IT
  - Software or software publishing
  - Cybersecurity or encryption
- **There is little agreement amongst industrial base as to what codes they align with and some were not aware that NAICS drives a lot of NSA's market surveys**

Example: Cybersecurity Skills and NAICS and NSA Labor Categories Alignment

Skill/Function	Description	NAICS	NSA Labor Category	Comments
Anomaly Detection	Real time monitoring/detection schemes. Key for data mining	No Code	No	
Situational Awareness	Safeguard sensitive data, sustain fundamental operation, and protect infrastructure, and intrusion	No Code	No	Could fit under system administrator. Could also encompass logging and auditing analysis, and network intrusion
Cyber/Digital Forensics	Application of investigation and analysis techniques of data from any computing device	No Code	No	Includes evidence collectors and security analysts
Event Correlation and Management	Network management event correlation including surveillance and control procedures	No Code	No	Could fit under system administrator or situational awareness
Cyber Warning and Notification Specialist	Alert of warnings, threats, advisories for system(s) , networks, etc.	No Code	No	Requires training and certification
Cyber Threat Analysis	Visualization, Hackers, data investigators, data assessments	No Code	No	Board spectrum of skills; might want to sub-divide further
System Engineers/Integrators	Emphasis on networks, devices, and applications	541512	Yes	Description focuses on CAD systems integration
Modeling & Simulation	Critical infrastructures, attacks, defenses, and consequences	541330 – Engineering Services	Yes	
Mission IV&V	Concepts protocols, tools for information assurance and cybersecurity	No Code	Yes	NASA has IV&V Cybersecurity Program for Interns

SAMPLE: NEW NAICS CODES ALIGNED TO CYBER SERVICES

Sector:	Cyber	New NAICS 57
Subsector:	Infrastructure and Support	571
Group:	Securely Provision/ Operate and Maintain	5711

NAICS Industry	5711X
Systems Requirements Planning	57111
Technology Research and Development	57112
Systems Development	57113
Software Assurance and Security Engineering	57114
Network Services	57115
Information Assurance Compliance	57116
Assurance and Security Engineering	57117
Information Systems Security Operations	57118
US Industries	**57111X**

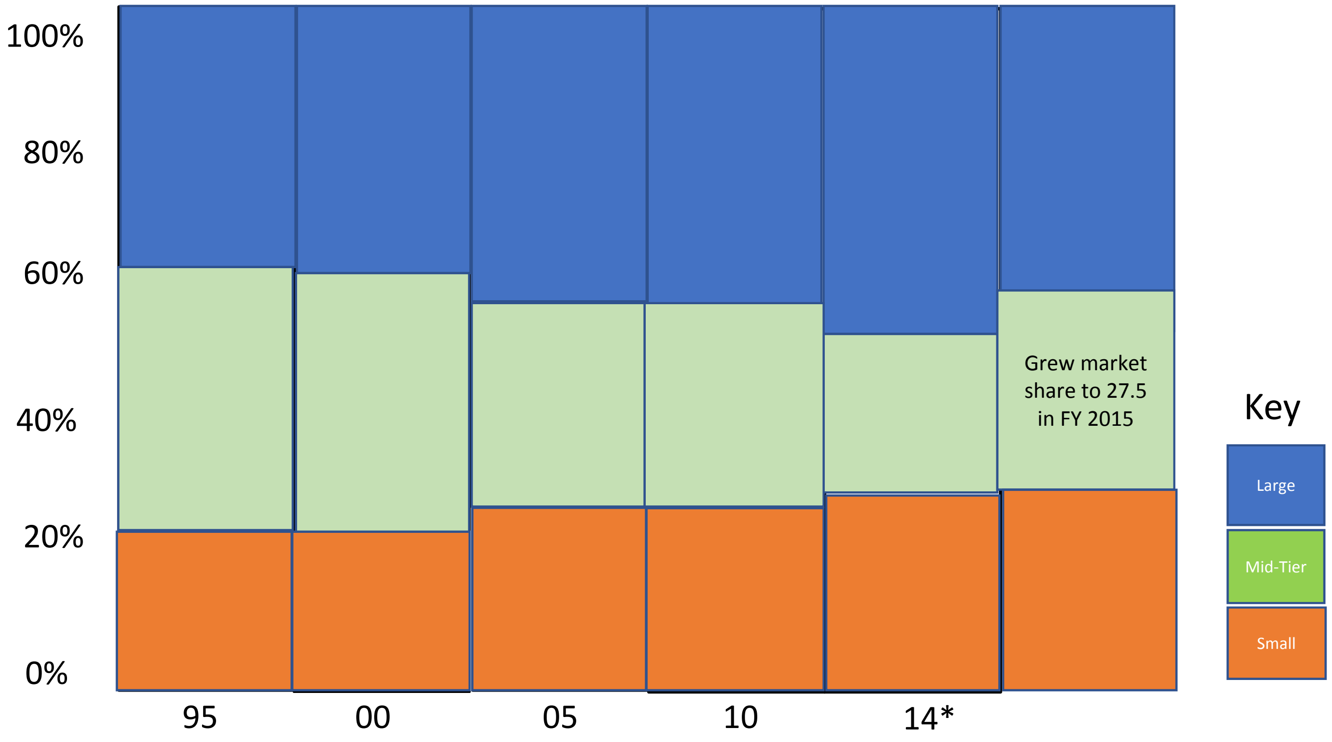
Sample of High Demand Cyber Skills and Functions*
Recovery and Reconstitution
Cyber Systems Administrator
Software Assurance and Security Engineer
System Security Architecture
System Security Analysts
Data Manager /Administrator

- Phase 2 Skills and Functions Aligned to Cybersecurity Workforce Framework

Market Dynamics

- **Mid-tier identification is complicated because differ in size, ownership, and valuation**
- **US Government needs to address in order to ensure the health of its industrial base and access to it**
- **US Government incentivizes small companies to succeed but has no support for their emergence into mid-tiers**
- **Some examples:**
  - SOTERA
  - Cybercore Technologies
  - PRAXIS Engineering
  - VanDyke Technology Group
  - ISS
  - Artic Slope/Vistronix

Mid-Tier Companies, 1995 to 2015



Grew market share to 27.5 in FY 2015

Sources: Emily Maltby, Contractors Find Gains Hard to Hold, Wall Street Journal, 3 Nov. 2011; Center For Strategic Studies, Defense Industrial Base Studies, 2011; Paul Murphy, Are Mid-Tier Contractors at a Disadvantage, Bloomberg Report, July 13, 2016

- 2014 assessment is estimated
- Shrinkage also attributed to acquisitions by large companies, and venture and equity investors

Criteria

- Utilize Small Business Set Asides as a potential mechanism to gain greater access to cybersecurity mid-tier companies
- No Federal law changes – no need to involve Congress
- No changes to existing FARS/DFARS
- Supporting legislative language is acceptable/desirable
- Support from DoD and ODNI needed for external coordination with Office of Management and Budget (OMB)
- Identify mechanisms that NSA can utilize to improve access to its industrial base

New Definitions for Categorizing Companies

- Small Businesses: Federal/NAICS definitions of size, revenue, and set asides are maintained
- Transitioning “Tweens” – 1-6 years since small, no more than 3X small limits in size or revenues – incentivize teaming with small businesses and use 10 percent share of small business set aside to promote prime behavior (roughly $40 million to $150 in revenues)
- ”Mid-Tweens” – All businesses with revenues more than $150 million and less than $350 million in revenues in “tween” category; establish set aside from 5 to 10 percent of 65 percent of large company contracting to promote prime bid. Prime must team with smalls or similar size ”tweens”
- “Mature Tweens” – All businesses with more than $350 million and not to exceed $600 million in revenues; establish set aside between 6 and 10 percent based on “mid-tier” set aside. Prime must team with smalls or other mid-tier companies.

Options For Improving NAICS For Cybersecurity Products and Services

Option	Description	Evaluation	Congressional Action	DoD Implementation	NSA Implementation	Finding
1. Abandon NAICS and create new cybersecurity Classifications for products and services	DoD and NSA would cease using NAICS codes when buying cybersecurity products and services. A separate classification system would be developed	▪ US government would have to agree to new strategy ▪ Would require coordination and agreement to develop new code system ▪ Could take years to complete and get agreement within government ▪ Change government-wide acquisition practices for acquiring cyber capabilities ▪ Change FARs	Congressional coordination and approval likely but probably no legislation required	• Within its powers and authority develop new categories but not to abandon NAICS • Could do as a pilot but difficult with upcoming election timelines • Will need OMB approval and Congressional approval at least in language to change FARs.	• Would have to coordinate with DoD • Could do as a prototype • Would have to include DISA and CyberCom which will increase timelines	Too difficult in government's current acquisition environment and priorities
2. Develop a separate set of NAICS codes for Cybersecurity products and services	Develop a separate set of NAICS codes that are specific to cybersecurity products and services	• Would be easier than trying to update existent categories to include cybersecurity • Coordination and agreement with OMB • Still does not solve problem of describing end-to-end capabilities	• Congressional coordination likely but probably no legislation required • If could make case for how it improves access to STEM and industrial base would gain support	• Not sure within its authorities • At a minimum would have to coordinate with OMB • Could Initiate as a pilot /prototype	• Might be able to do as a prototype/pilot for just NSA • Would have to coordinate with DoD • Could include DISA and CyberCom at later time after initial list developed	Too difficult in government's current acquisition environment
3. Expand Current NAICS codes for IT and computer products and services to include cybersecurity	• Update IT and computer categories to includes cybersecurity. • Update would include updating IT and computer categories to reflect changes in technology and how products and services are acquired	• Update of IT and computer categories should occur regardless • Would require coordination with OMB ▪ Could be initiated and managed by DoD ▪ Does not solve end-to-end capability definition problem	• Congressional coordination likely but no legislation required • Congressional support likely if could should that would expand access to US industrial base in cyber arena	• Yes within its powers and authority to initiate at least a pilot/prototype • Could do as a pilot and accomplish before national elections and transition. • Has the ability to coordinate and work with OMB to get needed changes	• Would have to coordinate with DoD • Could do as a prototype • Could include DISA and CyberCom at a later time • Could provide basis for DoD to adopt and then work with OMB	

Options For Improving NAICS For Cybersecurity Products and Services

Option	Description	Evaluation	Congressional Action	DoD Implementation	NSA Implementation	Finding
4. Redefine NSA labor categories to focus on cybersecurity requirements for services; develop categories for cyber products that would enable greater specification for use in RFPs, market surveys, and RFIs.	• Continue use of current NAICS codes but • Redefine labor categories to include cybersecurity for services; develop categories for specific products that agency needs for cybersecurity • Purpose of labor categories would shift from cost controls to needed services	• Would be easier than trying to update existent NAICs codes or labor categories to include cybersecurity • Could do solely within NSA and be thought leader for DoD and IC	• No coordination or legislation required • Could make case for how it improves access to STEM and industrial base	• Would not have to be involved • NSA should show that it's a leader in improving its access to its industrial base and that DoD could utilize or adopt this approach	• Could be developed by a small group of industry and government • Within SAE responsibilities and authorities • Redefinition could be done within a few months; internal coordination could take longer.	Most feasible of options in terms of accomplishing because within agency's and SAE authorities and responsibilities
5. Combine Options 3 and 4	• Provide a broad outline of how current NAICS codes could include cybersecurity products and services • Initiate focused effort on redefining labor categories on including cybersecurity contractor workforce, and develop product categories	• Both activities could be done within NSA • Could share initiatives with DoD and get support as needed • Could take credit for new ways to access cyber industrial base	• Could share with appropriate congressional leaders and take credit for tackling cybersecurity issues	• Coordinate and get support but • NSA could do both initiatives. The NAICS update as a prototype/pilot to assist DoD and labor categories as way to immediately assist NSA and its industrial base	• NSA has complete control over its labor categories and could demonstrate leadership within community. • NAICs initiative could gain support with DoD and IC agencies	Best course of action

Recommendations on NAICS Categories

- **Utilize agency acquisition authorities to develop a "prototype(s)" acquisition**
- **Develop own set of NAICS codes for cybersecurity as part of "prototype" acquisition**
- **Way ahead**
  - Develop recommendations in report on NAICS codes
  - Utilize **agency authorities** to demonstrate the value of adding cybersecurity NAICS
  - Modify NAICS codes – too hard to abolish in current environment
  - Modify labor categories (where can) or create separate set of labor categories for cybersecurity services and products
  - Utilize approach as a prototype that DoD could adopt; ODNI will be of little value in this endeavor

Recommendations – Mid-Tier Companies

- Create small business set aside for cybersecurity services and products
- Use agency procurement authorities to include “mid-tier” criteria in small business cybersecurity requirements
- Use approach in several individual procurements and assess benefit in terms of qualified and available labor pool
- Assess “prototype” procurements to share with DoD and IC leadership and Congressional representatives with key cybersecurity and acquisition stakeholder groups in DoD

Conclusions

- Since 2012 threat has escalated and in all likelihood will continue to accelerate
- The government will not be able to recruit a qualified government cyber workforce or develop needed capabilities fast enough to meet the rapidly evolving cyber threat
- The government will be severely challenged in gaining access to the needed contractor cyber workforce and technologies if NAICS and government hiring practices for its contractor workforce are not addressed
- The government cannot rely solely on its traditional industrial base to meet these challenges
- Without modification the government's high reliance on NAICS structure and definitions will hinder its access to the cyber industrial base
- Government acquisition and procurement should be completely governmental

Back Up

FAR/DFAR Evaluation

- **Federal law says that there will be Small Business Programs but leave the size and dollar value up to the Small Business Administration (SBA)**
- **Federal Acquisition Regulation Title 48, Chapter 1, Subcharge D, Part 19.1, 19-102 lays out guidelines for Small Business Programs**
  - The SBA establishes small business size standards on an industry-by-industry basis (See 13 Code of Federal Regulations (CFR) Part 121)
  - NAICS codes are published by the SBA
  - NAICS codes are updated by the OMB through its Economic Classification Policy Committee every 5 years.
  - New NAICS codes are not available for use in Federal contracting until the SBA publishes corresponding industry size standards (see 19.102(a)(1))
- **A product or service can only be classified in one industry, whose definition best describes the principal nature of the product or service being acquired even though for other purposes it could be classified in more than one**
- **When acquiring a product or service that could be classified in two or more industries with different size standards, <u>contracting officers</u> shall apply the size standard for the industry accounting for the greatest percentage of the contract price**
- **<u>Class waivers may be requested for products by the contracting officer to the SBA; service waivers have less clarity</u>**

SBA RULES ON SERVICE CONTRACTS

- **Business must meet five criteria:**
  - Size standard for your industry
  - Operate for profit
  - Independently owned and operated
  - Based in the United States
  - Make contribution to US economy
- **Small business tied to small business NAICs codes that vary in size and dollar value (e.g., $15m to $38.5m to 1500 employees)**
  - Engineering and subcontracting services is $38.5m and 1500 employees
  - Engineering services is $38.5m with no employee size stated
- **Government agency handling procurement has authorities to tailor acquisition and procurement to ensure access to industrial base**
- **No NAICS exist for cybersecurity services**
- **Absence of NAICS provides NSA the ability to define cybersecurity service categories and criteria to gain access to qualified mid-tier companies**

NEW NAICS CODES FOR CYBER PRODUCTS

Sector:	Cyber	New NAICS	93
Subsector:	Cyber Security and Operations		931
Group:	Cyber Infrastructure Development		9311
NAICS Industry		9311X	
	Cloud Computing	93111	
	Data Center Development and Integration	93112	
	Cyber Monitoring and Recovery Tools	93113	
	Technology Research and Development	93114	
	Encryption and Decryption Technology	93115	
	Trusted Internet and Network Connections	93116	
	Access Identity Technologies	93117	
US Industries		93111X	

NEW NAICS CODES FOR CYBER PRODUCTS

Sector:	Cyber	New NAICS	93
Subsector:	Collect and Operate		933
Group:	Integrated Cyber Operations		9331

NAICS Industry	9331X
Tool Technology and Development	93311
Network Attack	93312
Signal Interference and Jamming	93313
Disruption Technologies	93314
Information Sharing	93315
Visualization	93316
Exploitation	93317
Data Structuring, Data Tagging	93318
US Industries	**93311X**