ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

BLANKROME
CELEBRATING 75 YEARS

ACC NCR Securing the Supply Chain for Government Contractors: Current Trends and Best Practices

Presented by:

Justin A. Chiarodo, Partner & Practice Chair, Blank Rome LLP

Robyn N. Burrows, Associate, Blank Rome LLP

Viet Tran, Director & Senior Counsel, Raytheon Technologies

Alicia K. Lynch, Senior VP & Chief Security Officer, Cognizant

July 21, 2021

Today's Speakers

Justin A. Chiarodo
Partner & Chair, Government Contracts, Blank Rome LLP
202.420.2706
jchiarodo@blankrome.com

Robyn N. Burrows
Associate, Government Contracts, Blank Rome LLP
202.420.2268
rburrows@blankrome.com

Viet C. Tran
Director & Senior Counsel, Cybersecurity, Raytheon Technologies Corporation
860.728.7030
viet.tran2@rtx.com

Alicia K. Lynch
Senior Vice President & Chief Security Officer, Cognizant
571.407.4497
Alicia.Lynch@cognizant.com

BLANKROME

Introduction

BLANKROME

Overview – a convergence of supply chain issues

- COVID-19
- National security concerns (supplier restrictions)
- Impacts of globalization
  - Semiconductors
  - High-capacity batteries
  - Pharmaceuticals and their active ingredients
  - Critical minerals and strategic materials
- Performance pressure and limitations on cost recovery
- Growing cadence of new threats and regulations (e.g., Cyber EO)

BLANKROME

Broad risk management considerations

- Enterprise-wide coordination
- Operational impacts
- Contractual and regulatory reporting
- Contracts and subcontracts management
- Balance of business and legal risks
- Insurance

BLANKROME

Issues Facing Gov’t Services and National Security Supply Chains

BLANKROME

Growing Threats from Bad Actors

- Continued evolution of cyber and supply chain threats
- 2020: $600B lost from cybercrime
- State Actors: e.g., China (Huawei, ZTE, Hytera), Russia (Kaspersky)
- Criminal syndicates: Ransomware, IP theft, etc.

BLANKROME

Cyberattacks: Public Case Studies

- **USIS:** State sponsored hack impacting 25,000 gov't employees
- **Electronic Warfare Associates:** Ryuk ransomware attack on electronics supplier (attacker targets government and military entities)
- **BlueForce:** Defense contractor infected with Conti ransomware strain – Attack encrypts and threatens to publish data, and demands 17 bitcoins
- **Communications & Power Industries (CPI):** Defense electronics manufacturer's data was encrypted and held ransom through phishing attack. CPI paid $500k ransom
- **Tyler Technologies:** Software and IT service provider lost $1.5M from ransomware attack targeting phone and IT systems

BLANKROME

Potential Supply Chain Impacts under Cybersecurity EO

BLANKROME

President Biden's Cybersecurity Executive Order

- **What: New Cyber and Software Security Regulations**
  - Responding to: SolarWinds, Colonial Pipeline, and MS Exchange
  - Sets in motion major FAR revisions
- **Who:** All government contractors
- **When:** Rulemaking starting mid-July 2021
- **Takeaways:**
  - Expect DFARS Cyber-like standards in civilian procurements
  - Enhanced & standardized cyber reporting requirements
  - Big impacts on software security and incident reporting

BLANKROME

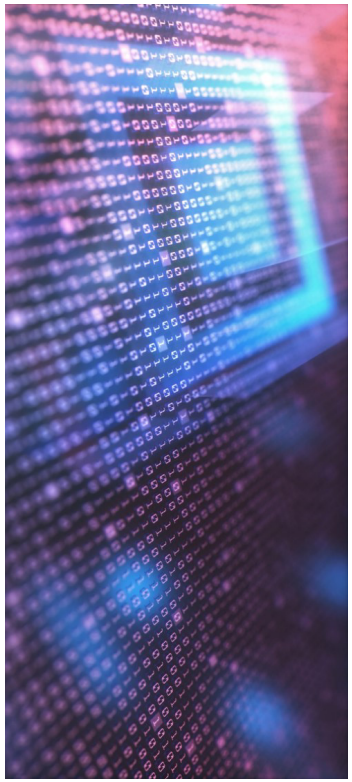
What does the EO cover?

- Cyber incident reporting and detection requirements
- Modernized cybersecurity standards
- Software security requirements
  - New NIST definition of “critical software”
- Cybersecurity safety review board (and event log)
- “Playbook” for cyber incident responses

BLANKROME

Practical Takeaways

- Civilian agency contractors will need to catch up
  - Begin planning now for CMMC-like regime
- Uniform requirements could ease regulatory burden
- Cybersecurity evaluation factors?
- Questions around immunity and proprietary information



BLANKROME

Current Supplier Exclusion Trends

BLANKROME

The landscape

- **Move away from Agency-by-Agency approach**
- **Federal Acquisition Supply Chain Security Act of 2018**
  - Created Federal Acquisition Security Council (FASC)
  - Up to now, no centralized body to address problematic suppliers
- **Supply Chain Risk Management (SCRM) Task Force**
- **Government-wide supplier bans**
  - Kaspersky Ban (2019)
  - Section 889 (Huawei, Hytera, Dahua, etc.) (2020)

BLANKROME

Kaspersky Lab Ban

- Kaspersky Lab ties to Russia's Federal Security Service
- FAR 52.204-23 bans cybersecurity products from Kaspersky Lab
- Kaspersky litigates ban as unconstitutional (but loses)

BLANKROME

Section 889 – Chinese Telecom Ban

- Prohibits *selling* (Part A) or *using* (Part B) "covered technology"
  - 5 manufacturers (Huawei, Hytera, ZTE, Dahua, Hikvision) + affiliates/subs
- Currently awaiting further Part B rulemaking
- Open questions:
  - What is "use"?
  - Telework equipment?
  - Overseas telecom?
- Case Study: Aventura Technologies

BLANKROME

Best Practices for Section 889 compliance

- **Document the "reasonable inquiry"**
  - Technology inventory
  - Review supplier information
  - Risk based approach
  - "Reasonable inquiry" to include publicly available info?
- **Document training**
  - "Regulatory familiarization" presumed
  - Include CTO, procurement department, and contracts managers
- **Prepare for potential extension to domestic subs + affiliates**

BLANKROME

Emerging Supply Chain Issues

BLANKROME

Issue 1: Cybersecurity Maturity Model Certification (CMMC)

- Interim rule released September 2020; awaiting final rule
- Key areas:
  - NIST assessments and SPRS
  - Identifying and marking CUI

BLANKROME

Cybersecurity Maturity Model Certification (CMMC)

- Are small/medium contractors ready?
  - 28% can't meet Level 1
  - 48% have "severe vulnerabilities"
  - 10% have critical vulnerabilities and evidence of compromise
- Cost of CMMC
  - $150k - $300k per assessment
- Expansion to Civilian Agencies?
  - GSA incorporating CMMC language

BLANKROME

CMMC implementation challenges

- Which CMMC level and for whom?
- CMMC level for suppliers?
- Are no POAMs realistic?
- Cybersecurity as an evaluation factor?

BLANKROME

Issue 2: ICTS Transactions

- Commerce Dep't may limit information and communications technology and services (ICTS) transactions post-Jan. 19, 2021
- Covers: "Foreign adversaries" posing national security threat
- "Transaction" broadly defined
- 180-day security review process
- Tip: Review your supply chain to determine if you might be impacted

BLANKROME

Performance Challenges: COVID-19 and the Defense Production Act

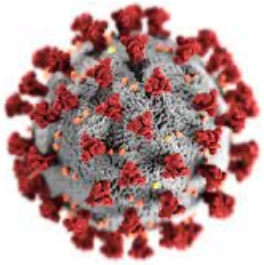
BLANKROME

Pressure on contractors

"Yes, there's a global pandemic, but I need this now"

"No, we won't pay you more for [x]"

- Recent issues
  - Increased use of Defense Production Act to meet critical needs
  - Challenges for cost-recovery under COVID-19 claims



BLANKROME

Issue 1: Defense Production Act of 1950

- Allows POTUS to mobilize industry in service of:
  - national defense; homeland security; emergency prep; public health
- Implementing regulations at 15 CFR 700 (Commerce Dep't)
- Allows USG to give priority to "rated orders"
- Companies prioritize rated orders over all other orders
- Immunizes contractors for breach of K stemming from delays

- **Key tip: close attention to rated order management**

BLANKROME

Priorities and allocations systems

Four elements for binding rated order (see 15 CFR 700.12)

1. The “DX” or “DO” priority rating and program designation
2. A specific required delivery date
   - this date cannot be sooner than the actual need
   - a “ship by” date also does not meet this requirement
3. A written or digital signature of authorized employee
4. A DPA regulatory statement…

BLANKROME

DPA statement

"This is a Rated Order certified for national defense use, and you are required to follow all the provisions of the Defense Priorities and Allocations System regulation (15 CFR Part 700)."

BLANKROME

DPA Compliance obligations

- Recipient of **proper** rated order has 10 days to accept or reject it
  - 15 CFR § 700.13(a)
- Recipient must **reject** order if:
  - Co. cannot fulfill the order by the date specified with appropriate priority
    - Must give issuer the earliest delivery date, and offer to accept for that date
  - The issuer's Rated Order would conflict with an existing Rated Order
    - Again, Company must give the issuer earliest delivery date and offer to accept
- Contractor may request any delivery date needed to meet own orders
  - Note: impossible date will result in the rejection of the Rated Order

BLANKROME

Issue 2: Cost recovery mechanisms

- **Changes Clause (*e.g.*, FAR 52.243-1)**
  - The big one: may cover costs stemming from USG direction to alter or stagger work hours, provide more personnel, use more costly procedures, use procedures requiring additional training for personnel, provide personal protective equipment, or perform additional cleanings
  - Agency guidance a key guidepost
- **Stop Work Order Clause (FAR 52.242-15)**
  - Costs stemming from the USG's direction to stop work generally recoverable
  - May include the cost of "idle time" (outside of Section 3610 of the CARES Act)
- **Delay of Work Clause (FAR 52.242-17)**
  - Where USG causes a delay, the resulting costs (e.g., increased material costs) may be recoverable
- **Note:** Excusable delays clause (FAR 52.249-14) provides time, not $$$

BLANKROME

Timing is key

- **Changes Clause (*e.g.*, FAR 52.243-1)**
  - Assert within 30 days of receipt of written change order
  - Exception if CO decides facts support delay (if before final payment)
- **Stop Work Order Clause (FAR 52.242-15)**
  - Assert within 30 days of end of work stoppage period
- **Delay of Work Clause (FAR 52.242-17)**
  - Notify CO within 20 days of the triggering event giving rise to delay
  - Must assert claim $$$ in writing as soon as practicable (and before final pay)
- **Don't forget about suppliers….**

BLANKROME

Cautionary tale: Pernix Serka

- ***Pernix Serka Joint Venture v. Sec'y of State***
- **Case No. 20-2153 (Fed. Cir. June 9, 2021)**
  - CBCA denies $1.25M claim re: Ebola outbreak; Fed. Cir. upholds
    - No order to continue performance despite dangerous conditions
    - Excusable delays clause **provides time, but not money**
  - Shows need for a USG-directed "change" for COVID-19 claims
- Reinforces importance of USG direction

PERNIX | serka
Joint Venture

BLANKROME

Risk Mitigation Strategies

BLANKROME

Indemnity, Insurance, and Suppliers

- Evaluate current subcontractor and vendor agreements
  - Critical vendors may be more vulnerable to cyberattacks
  - Do you have appropriate risk allocation/indemnity provisions?
  - Can you audit your suppliers?

- Cybersecurity/business interruption insurance
  - Cyber risks typically excluded from most policies
  - Premiums based on insured's level of self-protection
  - Costs for data recovery, ransom payments, and loss of income
  - COVID-19 business interruption claims a mixed bag

- Identify and actively manage critical suppliers

BLANKROME

Today's Speakers

BLANKROME

Justin A. Chiarodo

Partner & Chair
Government Contracts Practice
Blank Rome LLP

202.420.2706
jchiarodo@blankrome.com

1825 Eye St, NW
Washington, DC 20006

Justin Chiarodo is a Partner and Chair of the Government Contracts Practice Group at Blank Rome. Justin's experience extends to the full range of issues contractors encounter in the public sector marketplace, including bid protests, government investigations, contract claims and disputes, cost accounting and audit matters, regulatory compliance, mergers and acquisitions, suspension and debarment, and False Claims Act defense.

Justin leads a team of 25 professionals in his role as Practice Chair, with a singular focus on client service.

.

BLANKROME

Robyn N. Burrows

Associate
Government Contracts Practice
Blank Rome LLP

202.420.2268
rburrows@blankrome.com

1825 Eye St, NW
Washington, DC 20006

Robyn Burrows is an Associate at Blank Rome focusing her practice on all aspects of government contracts. She is experienced in litigating complex government contracts claims and disputes. Robyn regularly provides counseling on matters relating to regulatory compliance, with a particular focus on emerging cybersecurity and supply chain issues, as well as domestic preferences and cost/pricing issues. Robyn has also assisted clients with numerous bid protests before the Government Accountability Office and U.S. Court of Federal Claims.
.

BLANKROME

Viet C. Tran

Director and Senior Counsel for Cybersecurity, Raytheon Technologies Corporation

860.728.7030
viet.tran2@rtx.com

Office of the General Counsel
10 Farm Springs, 10FS-2
Farmington, CT 06032-2568

Viet Tran is Director and Senior Counsel for Cybersecurity at Raytheon Technologies Corporation where he advises the company and its businesses on all aspects of cybersecurity law, focusing on compliance and incident response.

Most recently, prior to the merger of United Technologies Corporation and Raytheon Company in 2020, Viet served as Director and Senior Counsel for Compliance at UTC where he advised the company's Digital Technology and Engineering functions on a variety of compliance matters, including cybersecurity and export controls.

BLANKROME

Alicia K. Lynch

Senior Vice President, Chief Security Officer, Cognizant

571.407.4497
Alicia.Lynch@cognizant.com

55 Hudson Yards
26th Floor
New York, NY 10001

Alicia Lynch joined the Cognizant team in July bringing over 30 years of intelligence, security, and cyber experience with the Department of Defense, the Defense Contracting community and the private sector. Alicia retired as a Colonel from the US Army in 2012 where she served as both an Intelligence and Cyber Officer. Alicia earned respect as a dynamic leader of soldiers in combat as well as garrison environments in assignments around the world. As both a qualified intelligence professional and cyber specialist, she served in every echelon from Company to National while leading units from team-sized to commanding a Brigade. Since 2012 she has leveraged her technical experience in commercial executive level positions focused on cyber and security. She has recently held titles including the Chief Information Security Officer at SAIC, Deputy Chief Information Security Officer at Accenture Federal Services, and VP of Enterprise Solutions at a Cyber startup. Alicia is an active member and supporter of many organizations such as WashingtonExec CISO Council where she served as the founding Chairwoman and is on their Women's Leadership Council, as well as the Northern Virginia Technology Council where she is on the Cybersecurity & Privacy Committee, and Zooms CISO Council. Alicia is also a Fellow at the Center for Strategic and International Studies (CSIS) in the Women's Global Leadership Program. She has been named numerous times to the Top CISOs to watch in Washington, DC.

BLANKROME

To stay on top of these issues…

- Click and subscribe to our *Government Contracts Navigator* blog: **https://governmentcontractsnavigator.com**

- Follow us on **@GovConBR**

BLANKROME