Cyber Preparedness

> A Proactive Response to Infiltration

Colin McKinty
Vice President, Cyber Strategy for the Americas
colin.mckinty@baesystems.com

April 2016

BAE SYSTEMS
INSPIRED WORK

Cyber Preparedness

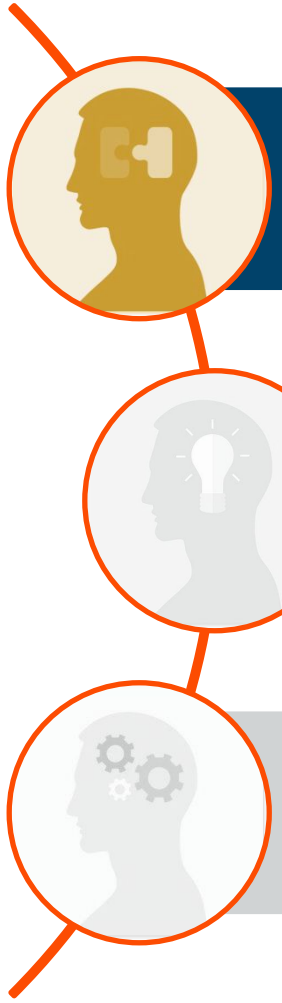
How To Get Started

Take A Proactive Stance

Be Ready to Respond

BAE SYSTEMS
INSPIRED WORK

Cyber Preparedness



How To Get Started

Take A Proactive Stance

Be Ready to Respond

BAE SYSTEMS
INSPIRED WORK

Where Does Cyber Preparedness Begin?

Technology?

Security team?

Processes?

BAE SYSTEMS
INSPIRED WORK

It starts with The Board.

It is driven by a culture where cyber risk is addressed as part of operational risk

BAE SYSTEMS
INSPIRED WORK

Why Should They Care?

BAE SYSTEMS
INSPIRED WORK

The Obvious

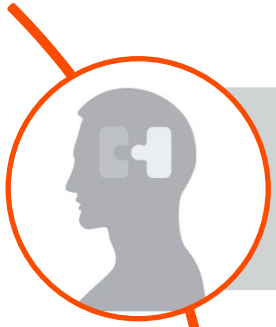
BAE SYSTEMS
INSPIRED WORK

Reducing Risk.

Enables Growth.

BAE SYSTEMS
INSPIRED WORK

Cyber Preparedness



How To Get Started

Take A Proactive Stance

Be Ready to Respond

BAE SYSTEMS
INSPIRED WORK

- Fire started in a NJ home last year
- A driver saw the fire and banged on the front door until someone answered
- The alarms went off -- afterward
- The family inside escaped
- Fireman eventually got control
- Happy ending … but what if the driver did not stop?
- Also, almost one year later, re-construction is just starting

BAE SYSTEMS
INSPIRED WORK

Effective Smoke Detection

- Consider where you replace them
- Ensure the batteries work
- Monitor and maintain

BAE SYSTEMS
INSPIRED WORK

Have a Plan for When the Alarm Goes Off

- Think of this as Incident Response
- The value of knowing someone is looking after you … ready to bang on your door when fire starts

BAE SYSTEMS
INSPIRED WORK

- What if there's a "fire" in your network?
- What if the alarms don't go off right away or if you don't have the right alarms in place?
- What kind of damage could that do if your business took a year to get back to normal?
- Also, consider the scenario where your entire operation "burns to the ground"

BAE SYSTEMS
INSPIRED WORK

Hierarchy of Security Needs

To be fully prepared and avoid disasters:

- Detect new, hidden threats
- Effectively and efficiently respond
- Reduce the time & resources required in the detection to resolution phase

BAE SYSTEMS
INSPIRED WORK

Prevention: Still Important

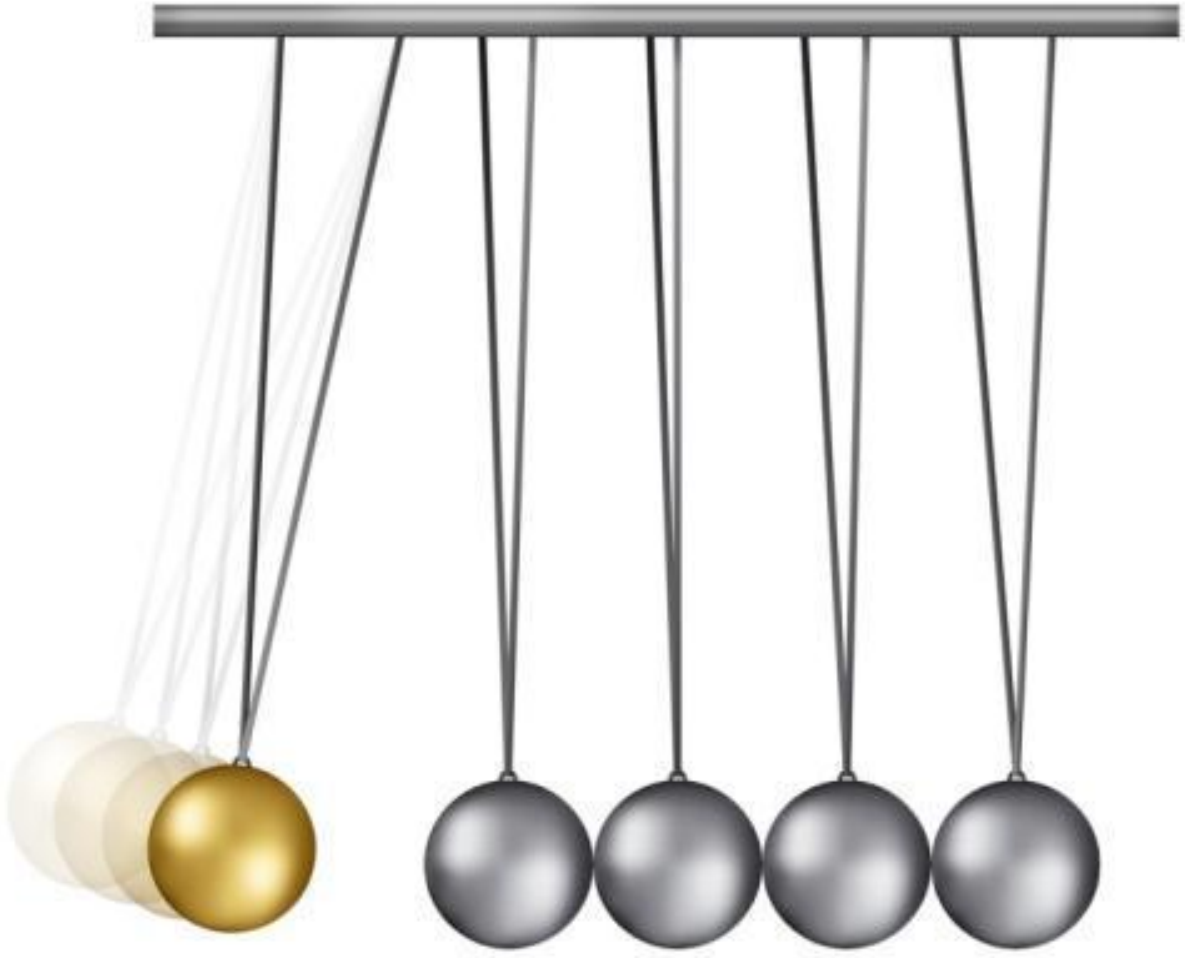
BAE SYSTEMS
INSPIRED WORK

Balancing Spend Allocations

Prevention

Detection

Response



BAE SYSTEMS
INSPIRED WORK

The ability to respond to an incident is only as good as an organization's ability to …

detect the incident.

BAE SYSTEMS
INSPIRED WORK

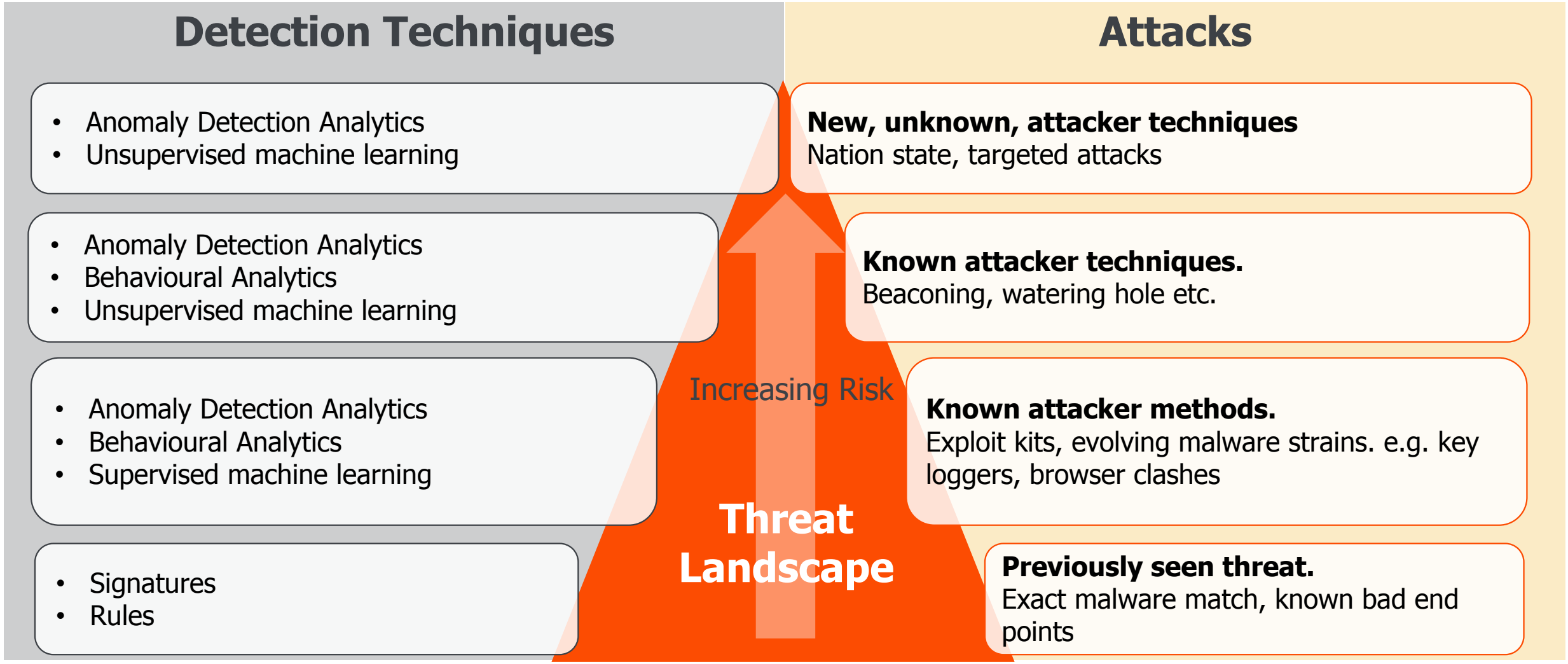
Detection

> Why It's Challenging

- Too many bad guys/attacks
- Bad guys don't want to be found
- Attacks take new forms every day
- Sophisticated APT and targeted attacks routinely circumvent existing security defenses
- The longer they stay undetected, the greater the financial damage and sensitive data loss

BAE SYSTEMS
INSPIRED WORK

Analytics Techniques



BAE SYSTEMS
INSPIRED WORK

Characteristics of Behavioral Analytics

Potentially bad vs known bad

Enduring vs brittle

Risk based vs binary

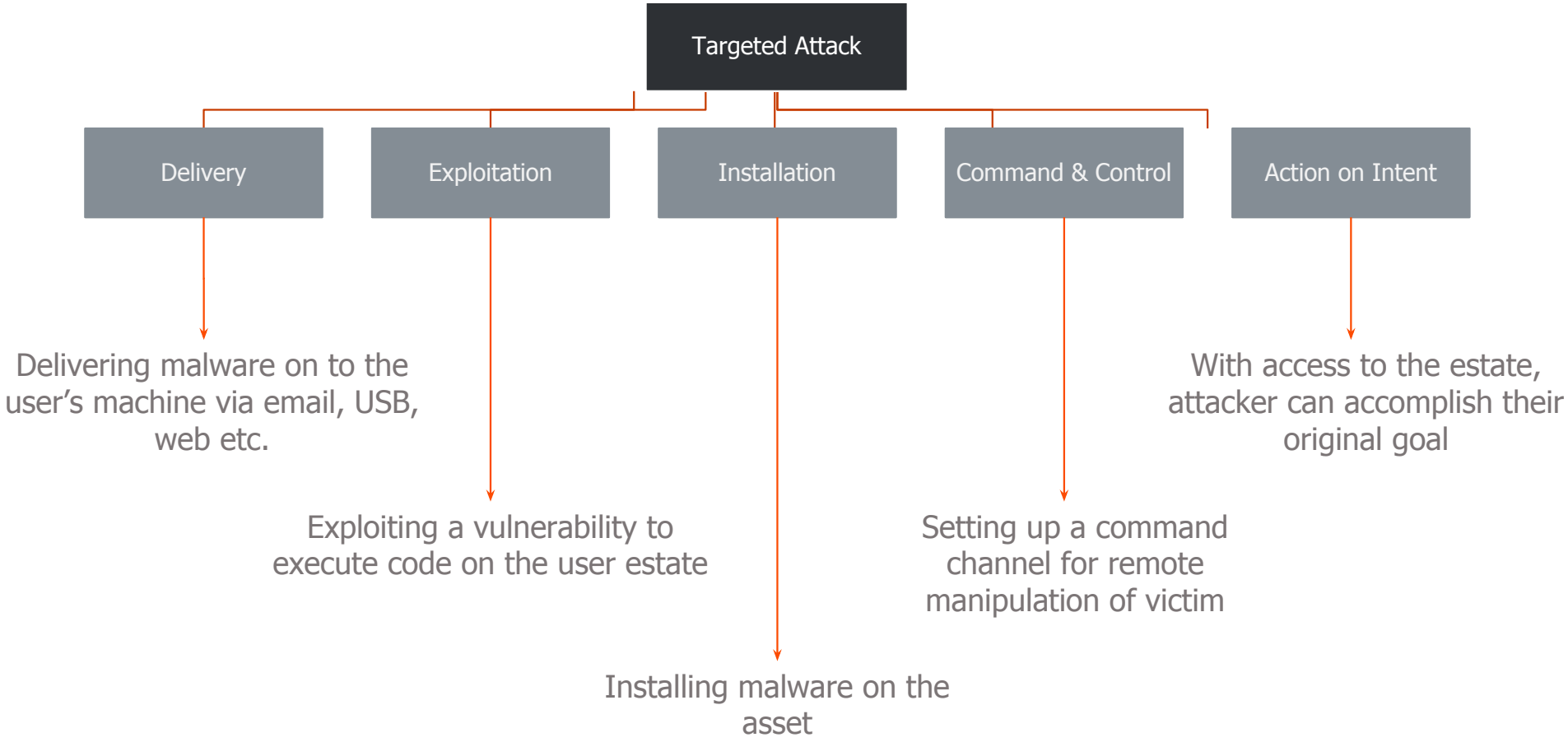
Time range vs point in time

General vs specific case

BAE SYSTEMS
INSPIRED WORK

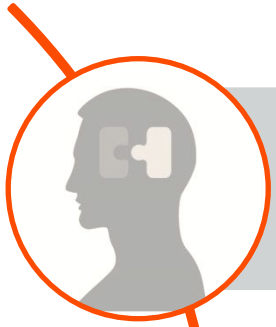
Detection needs to driven by a Threat model

Analytics are categorised by 'attack technique'. These are the stages an attacker has to go through to successfully complete an attack on a network.



BAE SYSTEMS
INSPIRED WORK

Cyber Preparedness



How To Get Started

Take A Proactive Stance

Be Ready to Respond

BAE SYSTEMS
INSPIRED WORK

Response

BAE SYSTEMS
INSPIRED WORK

Having proper analysis capabilities requires both trained personnel and the proper tools to perform the analysis.

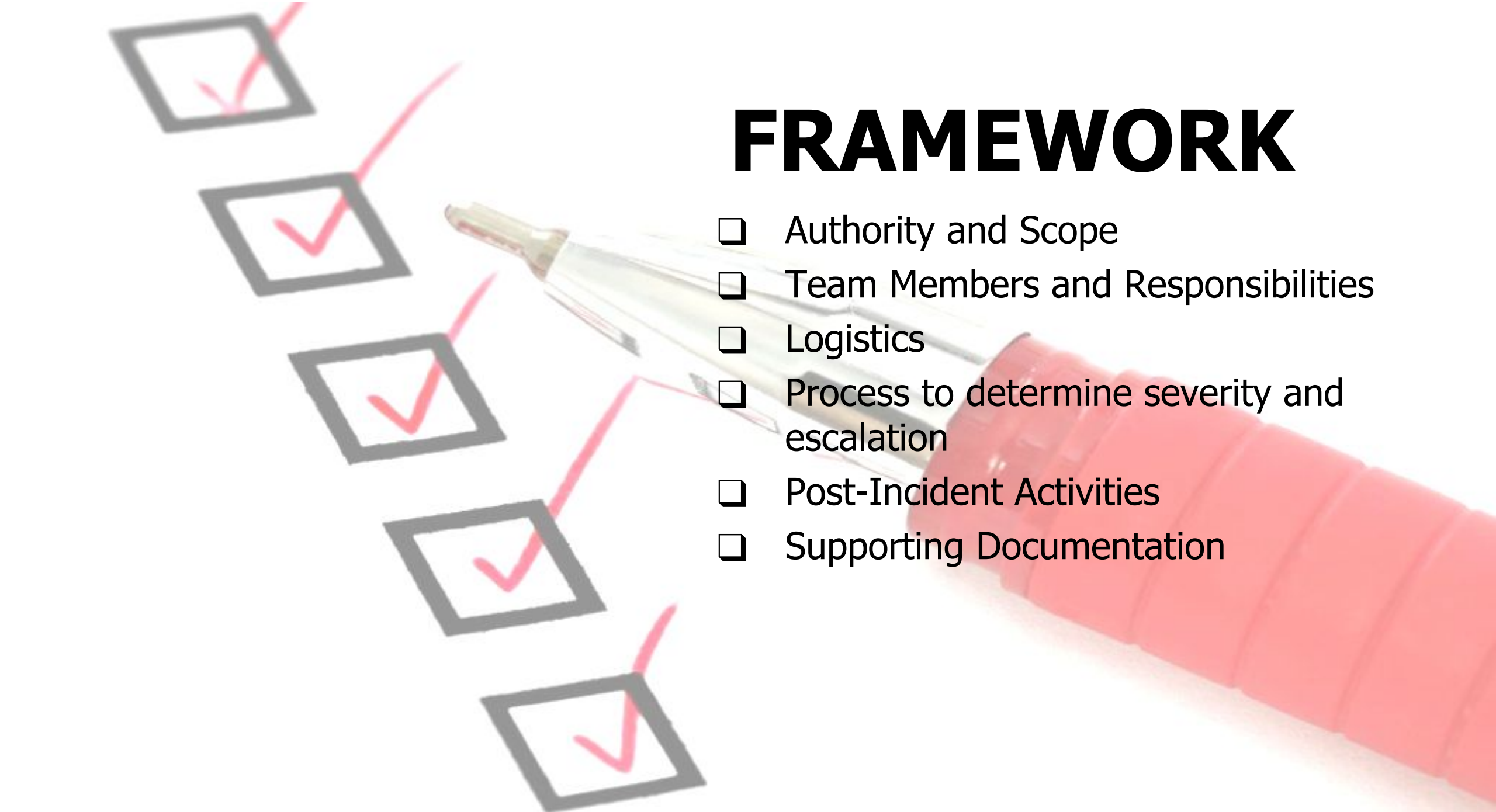
BAE SYSTEMS
INSPIRED WORK

A PLAN
VS
A FRAMEWORK

"No plan of operations
extends with certainty
beyond the first encounter
with the enemy's main strength"

-- Helmuth Karl Bernhard Graf von Moltke

BAE SYSTEMS
INSPIRED WORK



FRAMEWORK

- ❑ Authority and Scope
- ❑ Team Members and Responsibilities
- ❑ Logistics
- ❑ Process to determine severity and escalation
- ❑ Post-Incident Activities
- ❑ Supporting Documentation

The most critical component in any Incident Response Practice …

Authority and backing from executive management.

BAE SYSTEMS
INSPIRED WORK

IR Team

- Primary team
- Extended team
- Third parties

BAE SYSTEMS
INSPIRED WORK

Primary

- Security Team
- IR Lead
- Operations Team
- Service Desk Team

BAE SYSTEMS
INSPIRED WORK

Extended

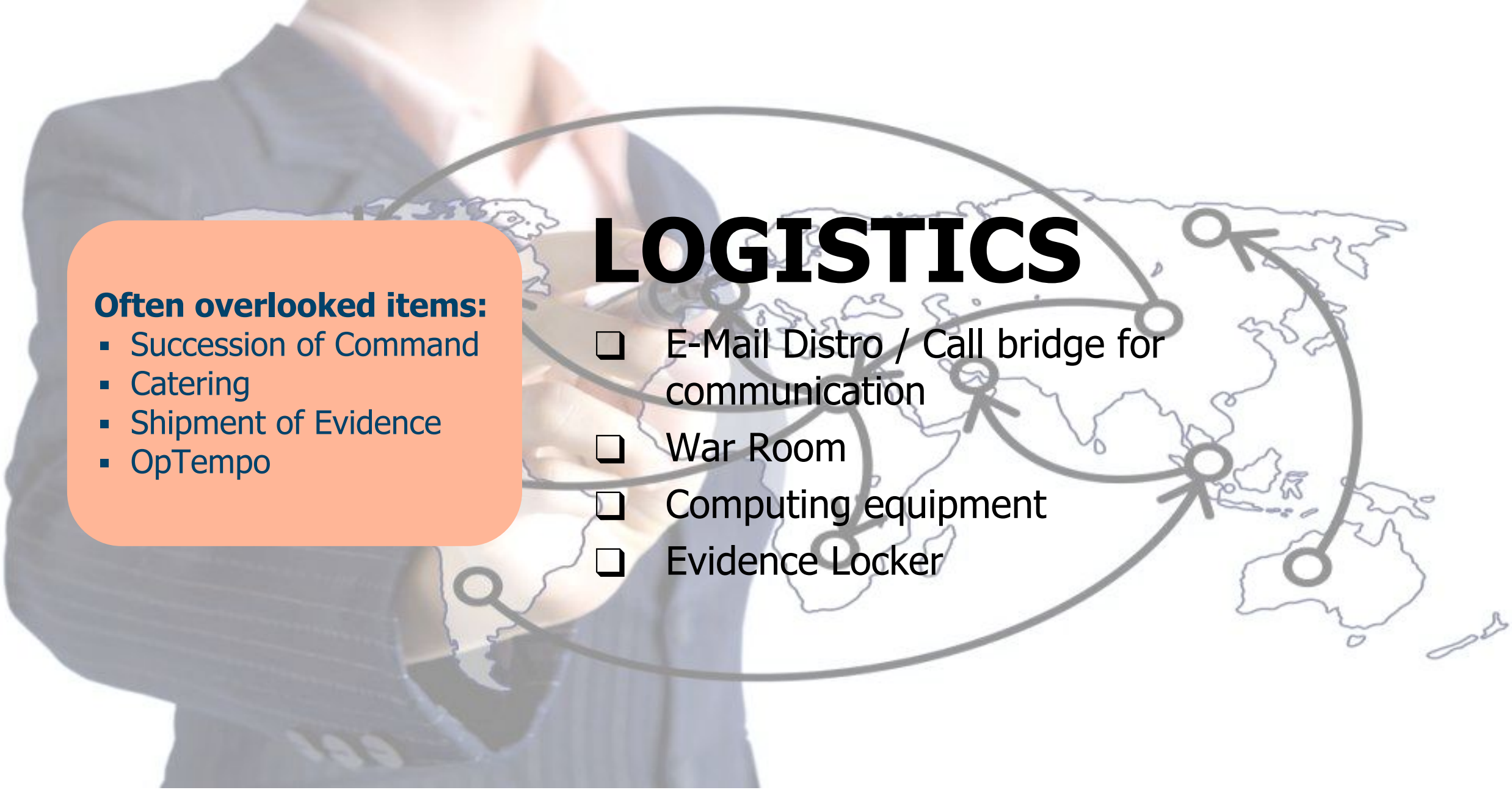
- Executives
- Legal
- Communications
- Human Resources
- Compliance
- Physical Security

BAE SYSTEMS
INSPIRED WORK

3rd Parties

- Outsourced IT (help desk, server support)
- Forensic Firms
- ISPs
- Legal Counsel
- Law Enforcement
- Public Relations Teams

BAE SYSTEMS
INSPIRED WORK



Often overlooked items:

- Succession of Command
- Catering
- Shipment of Evidence
- OpTempo

LOGISTICS

- ❑ E-Mail Distro / Call bridge for communication
- ❑ War Room
- ❑ Computing equipment
- ❑ Evidence Locker

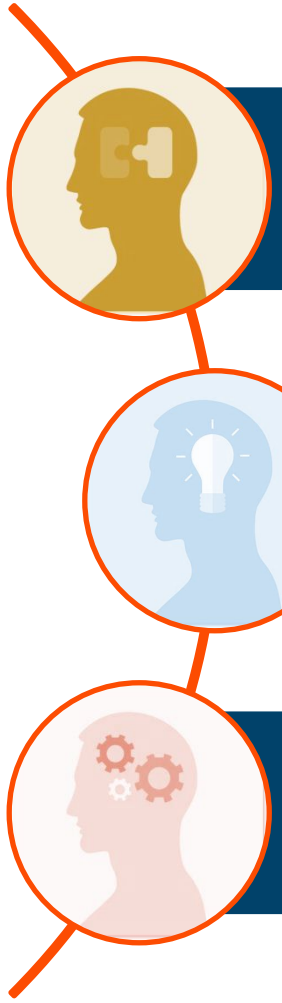
BAE SYSTEMS
INSPIRED WORK

Testing Incident Response

- ❑ High Level Audit
- ❑ Objective Based Assessment
- ❑ Table top Exercise
- ❑ War Game

BAE SYSTEMS
INSPIRED WORK

Cyber Preparedness – Key Takeaways



Begins With Preparedness Culture

Balancing Act; Varied Techniques

Turn IR Plan Into an IR Framework

BAE SYSTEMS
INSPIRED WORK

Thank You

BAE SYSTEMS
INSPIRED WORK

Q&A

BAE SYSTEMS
INSPIRED WORK

BAE Systems
Surrey Research Park
Guildford
Surrey
GU2 7YP
United Kingdom

T: +44 (0)1483 816000
F: +44 (0)1483 816144

BAE SYSTEMS
INSPIRED WORK

FREEDOM OF INFORMATION ACT

This document (<projectreference><documentnumber>) contains confidential and commercially sensitive material which is provided for the Authority's internal use only and is not intended for general dissemination.

The information contained herein pertains to bodies dealing with security, national security and/or defence matters that would be exempt under Sections 23, 24 and 26 of the Freedom of Information Act 2000 (FOIA). It also consists of information which describes our methodologies, processes and commercial arrangements all of which would be exempt from disclosure under Sections 41 and 43 of the Act.

Should the Authority receive any request for disclosure of the information provided in this document, the Authority is requested to notify BAE Systems Applied Intelligence. BAE Systems Applied Intelligence shall provide every assistance to the Authority in complying with its obligations under the Act.

BAE Systems Applied Intelligence's point of contact for FOIA requests is:

Chief Counsel
Legal Department
BAE Systems Applied Intelligence
Surrey Research Park
Guildford Gu2 7YP
Telephone 01483 816082

BAE SYSTEMS
INSPIRED WORK