International Telecommunication Union

Workshop on Addressing Security Challenges on a Global Scale

Session 5.1:

Global Cybersecurity Information Exchange Framework

Challenges in Sharing Security Information

Ian Bryant, NEISAS Project

7 December 2010

ITU, Geneva, CH

neisas

National & European Information Sharing & Alerting System

ms3i

[IAP_2010_G_057]

National & European Information Sharing & Alerting System

Messaging Standard for Sharing Security Information

Project JLS/2007/EPCIP/007 was co-funded by the European Commission (EC), Directorate General for Justice, Freedom and Security (DG JLS) as part of the "*European Programme for Critical Infrastructure Protection*" (EPCIP) Programme under the original title: "*Messaging standards for computer network defence warnings and alerts*"

It was performed with the support of the EC DG JLS "*Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*" Programme

Sharing Information in ISO/IEC 270nn Context

- The emergent body of ISO/IEC guidance on Information Security Management Systems (ISMS) is in the **270nn** Series

ISO International Organization for Standardization

IEC

- **270nn** assumes a uniform perception of risk, by implication even across multiple organisations
- **270nn** assumes all participants can be equally trusted
- **270nn** assumes all ISMS information is equally trustworthy
- **270nn** assumes that all risk managers can assess the effectiveness of all security controls

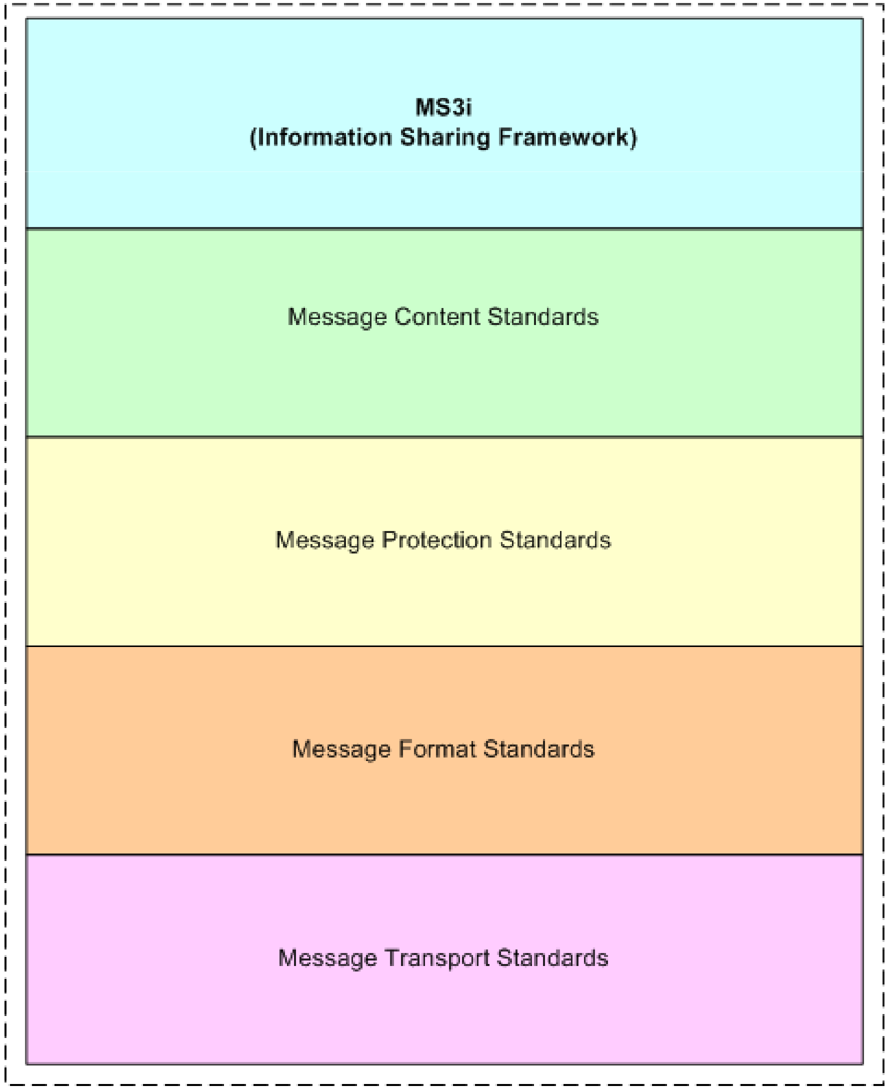
Standards for Information Sharing

- There **is** something special about trusted information sharing between organisations
  - Trusted Information Sharing needs **security management** of the sensitive **information exchanges** between organisations
- The EU funded MS3i and NEISAS Projects explored this topic area
- This work is forming the basis for a new Draft International Standard (IS): **ISO/IEC 27010**

National & European Information
Sharing & Alerting System

Standardisation: Layered Approach

- MS3i and NEISAS focus on Management Framework to support Sharing Security Information
- Expects to build upon a number of layered components for messaging information



MS3i
(Information Sharing Framework)

Message Content Standards

Message Protection Standards

Message Format Standards

Message Transport Standards

neisas
National & European Information Sharing & Alerting System

Standardisation: Existing Coverage

- Message Transport Standards
  - *De facto* adoption of (IETF) TCP/IP
- Message Format Standards
  - *De facto* adoption of (ISO/IEC) XML
- Message Protection Standards
  - *De facto* adoption of (W3C) XML-Sig / -Enc
- Message Content Standards
  - Mainly *de facto* adoption of (Mitre) C*E
- **ISO/IEC 27010** designed as capstone ***Information Sharing Framework*** for these layers

neisas
National & European Information Sharing & Alerting System

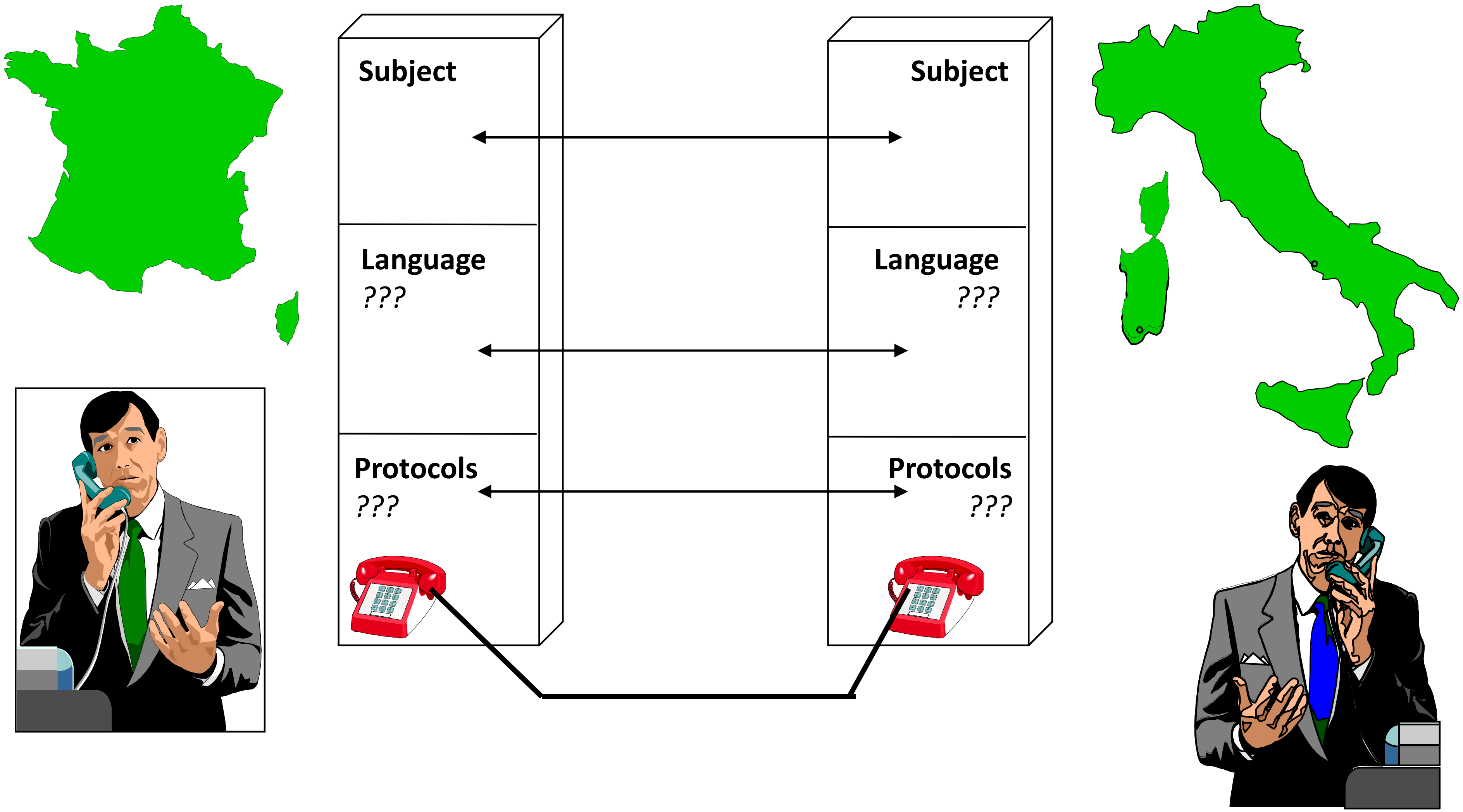
Information Sharing for Cybersecurity

In Cybersecurity context, **ISO/IEC 27010** needs to be considered in conjunction with other ISO/IEC efforts, in particular :

- **ISO/IEC 27032**: Guidelines for Cybersecurity
- **ISO/IEC 27035** (*+ t.b.c.*): Incident Management, Operation and Response
- **ISO/IEC 27037** (*+ t.b.c.*): Digital Evidence and Forensics

neisas
National & European Information
Sharing & Alerting System

Basic Implementation Challenges to Sharing



Subject

Language
???

Protocols
???

Subject

Language
???

Protocols
???

Perception: Cognitive Biases

- Cognitive biases are patterns of deviation in judgment that occurs in particular situations, which can be:
  - Examples of evolutionary mental developments
    - e.g. adaptations that lead to more effective actions or enable faster decisions
  - Lack of appropriate mental mechanisms
  - Misapplication of a mechanism that is adaptive under different circumstances
- Of particular relevance are Kahneman/Tverksy Heuristics (especially Anchoring, Availability and Representativeness)
- Cognitive Biases mean that differing people / communities will perceive **the same** information **in differing ways**

Perception: The Impact Fallacy

- Impact is a fundamental element of Information Security Risk Assessment
- Yet in many ways not suitable for Information Sharing
  - Unlikely to be a Generic Impact, but rather influenced by Environmental Factors (Organisation, Locale, Time)
  - Intrinsic modelling problems if Low Probability / High Impact: e.g. Taleb's *Black Swan*
  - Very susceptible to Cognitive Bias, in particular prior knowledge of others' assessment Situates the Appreciation by Anchoring

National & European Information
Sharing & Alerting System

Trusted Information Sharing Challenges

Challenges with modelling trust in (potentially *ad hoc*) NEISAS environments:

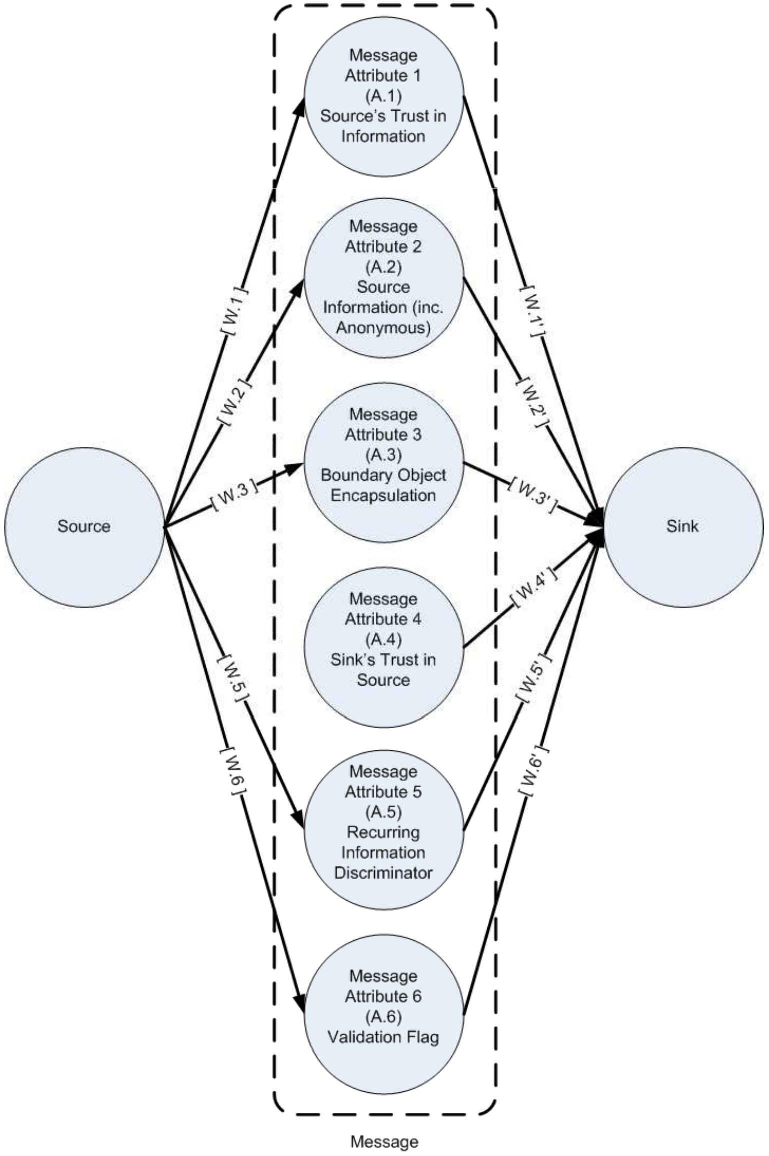
- The communities are not necessarily aligned to the natural “Circles of Trust”
- The communities may not share either a common language and/or ontology
- The communities **may not know** trustability of *ad hoc* partners

Trust: Specious Reinforcement

- Guglielmo Marconi conjectured in 1909 that any person could be connected to another by at most 5 people:
  - Issue also reflected by “Erdös Number”, “6 Degrees of Separation”, “Kevin Bacon Game”, “Small World problem”
- Empirical evidence is number of degrees of separation closer to 7:
  - Duncan Watts (2001) test with 48,000 emails found average number of intermediaries just over 6
  - Microsoft (2007) study of 30 billion instant messenger conversations found the average path length was 6.6
- Any model of Trust should not use linear weighting for additional instances (*de minimis* for larger values)

Trust: Derived Model (1)

- Recipient’s trust in received statement largely predicated on :
  - Trust in source / message
  - Source’s view of statement
- Model elements:
  - Originators of information should assign a degree of trust in information they publish
  - All information be clearly identified with the source, ideally using a structured data format
    - But should be support for anonymous reporting, from Safety world experience

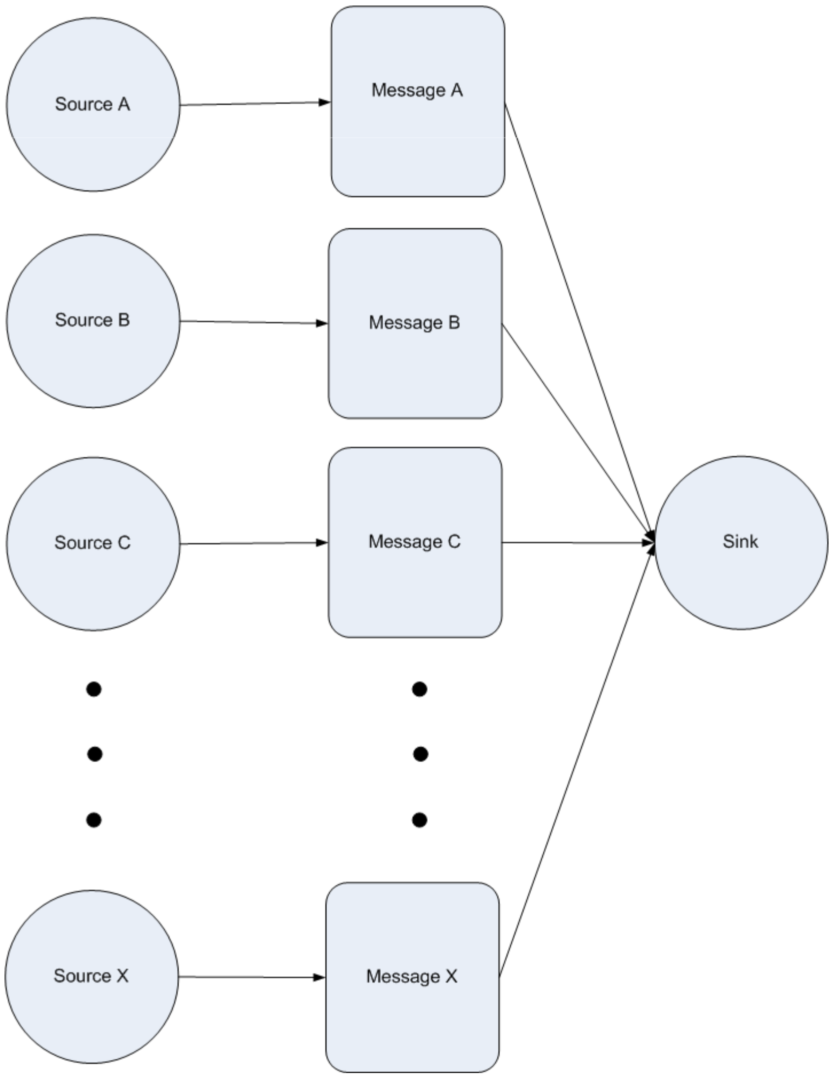

Message Attribute 1 (A.1) Source's Trust in Information
Message Attribute 2 (A.2) Source Information (inc. Anonymous)
Message Attribute 3 (A.3) Boundary Object Encapsulation
Message Attribute 4 (A.4) Sink's Trust in Source
Message Attribute 5 (A.5) Recurring Information Discriminator
Message Attribute 6 (A.6) Validation Flag
Source
Sink
[W.1]
[W.2]
[W.3]
[W.5]
[W.6]
[W.1']
[W.2']
[W.3']
[W.4']
[W.5']
[W.6']
Message

neisas
National & European Information
Sharing & Alerting System

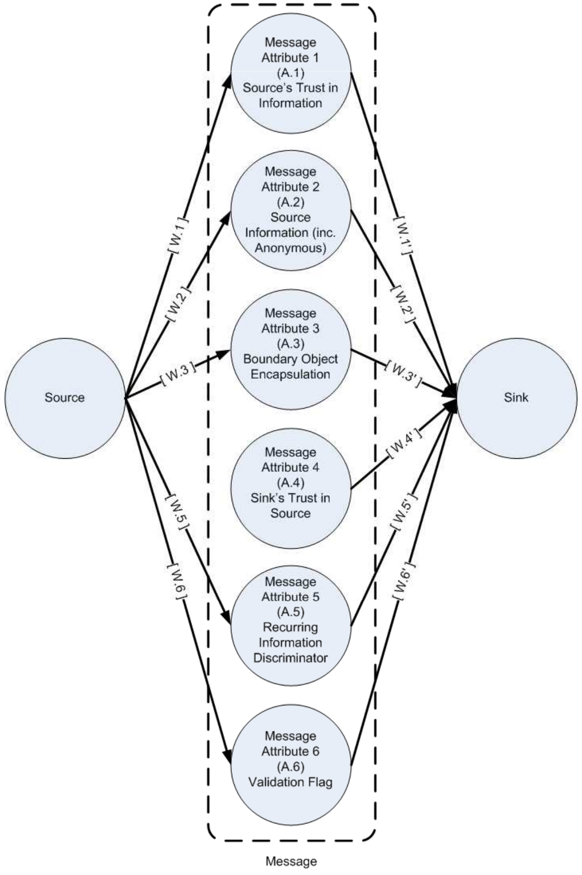
Trust: Derived Model (2)

Model elements (contd.) :

- Boundary Objects (structured information with mutual recognition across linguistic and domain boundaries) used to encapsulate information
- Both Originator and Recipient should assess how many times information previously received (to deal with Specious Reinforcement)
- Originator or Recipient verify information independently checked
- Recipients of information should assign a subjective rating of the source



Trust Metric: Shape Function


Source
Message Attribute 1 (A.1) Source's Trust in Information
Message Attribute 2 (A.2) Source Information (inc. Anonymous)
Message Attribute 3 (A.3) Boundary Object Encapsulation
Message Attribute 4 (A.4) Sink's Trust in Source
Message Attribute 5 (A.5) Recurring Information Discriminator
Message Attribute 6 (A.6) Validation Flag
Sink
[W.1]
[W.2]
[W.3]
[W.5]
[W.6]
[W.1']
[W.2']
[W.3']
[W.4']
[W.5']
[W.6']
Message

Matroid Algebra

$$U = \sum_{A}^{X} \frac{1 - e^{-\left(\frac{An.Wn'}{n}\right)k}}{e}$$

approximated as Weibull CDF

Pareto approach: perfection would need disproportionate effort, and may not be feasible

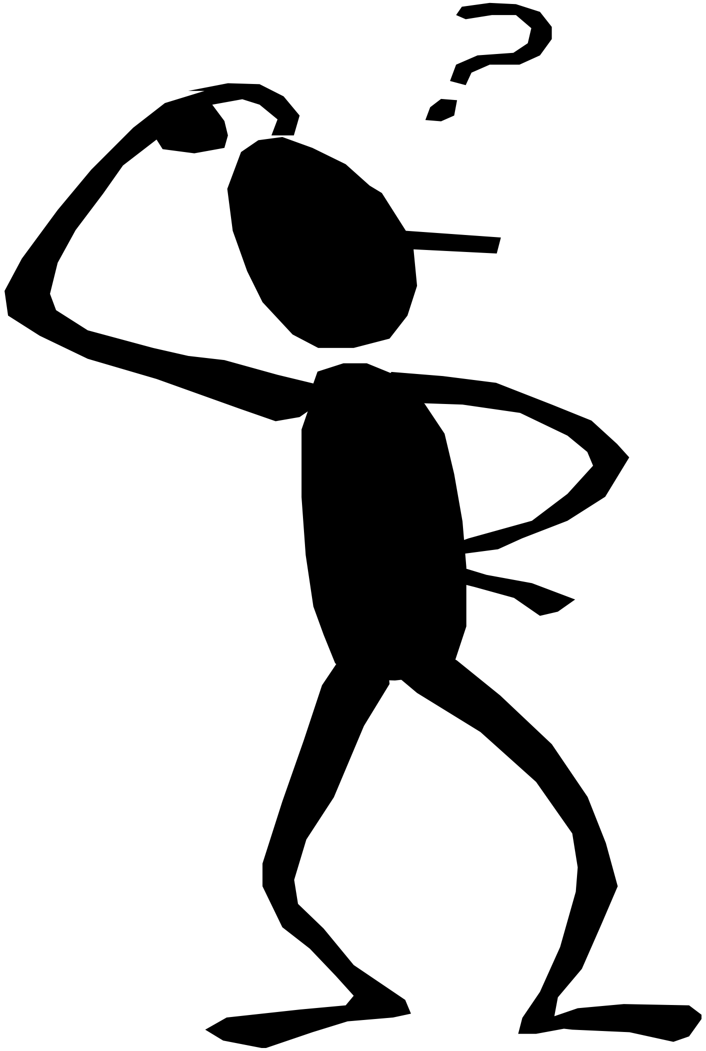
neisas
National & European Information
Sharing & Alerting System

Information Sharing: Proof of Concept

- Public / private sector Critical Infrastructure Protection (CIP) stakeholders want :
  - True exchange of information, not just ‘push’ portals
  - Owners to choose who can read information, including enforcing Traffic Light Protocol (TLP)
  - ‘Peer to Peer’ exchange with no central system
- NEISAS providing prototype trusted electronic information sharing National platform based on MS3i and 27010 for threat and vulnerability information
- Will also allow bilateral exchange at the European level between National platforms

neisas
National & European Information Sharing & Alerting System

Any Questions ?



National & European Information Sharing & Alerting System

Contact Details

Ian Bryant
Information Assurance (IA) Advisor

c/o NEISAS Project
Innovation Martlesham
Adastral Park
Martlesham Heath
Ipswich
Suffolk IP5 3RE
United Kingdom

ianb@neisas.eu

+44 75 9500 9715

www.neisas.eu