NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE

(NCIIPC)

OVERVIEW

- ICT Challenges
- CI vs CII
- NKN in the context of CII
- Framework for Evaluating and Enhancing Cyber Security in CII
- Outreach Programme

ICT – Todays Challenges

- Information and communication Systems converged
- The same communication media carries multiple data streams
- Exposure (Attack Surface) greatly enlarged
- Rapidly expanding infrastructure
- Hacktivists, “click to attack” etc
- Attackers can remain virtually untraceable

ICT – Todays Challenges (contd)

- Open to Supply Chain contamination
- Communication media is itself the target (DDoS)
- Dark Web Hosted Botnets

Effects of Cyber Attacks on CII

- Damage or Destruction of CII
- Disruption or Degradation of Services
- Loss of Sensitive / Strategic information
- Cascading Effect

THE SHORT POINT -
WHAT DOES (ALL) THIS TRANSLATE TO?

CRITICAL INFRASTRUCTURE (CI)

"Those facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation".

CRITICAL INFRASTRUCTURE (CI)

1. Energy
2. Transportation (air, surface, rail & water)
3. Banking & Finance
4. Telecommunication
5. Defence
6. Space
7. Law enforcement, security & intelligence
8. Sensitive Government organisations
9. Public Health
10. Water supply
11. Critical manufacturing
12. E-Governance

CHARACTERISTICS OF CII

- Complex
- Distributed
- Interconnected
- Interdependent

NKN In the context of CII

- Each of the foregoing is an attribute of NKN.
- NKN morphing from mainly infrastructure provider to provider of services
  - by virtue of the interconnect that it provides.
- May soon be viewed as a service, the availability of which will be increasingly critical for various organisations
- A stated design parameter is that NKN is specifically planned to match unknown future demands.

NCIIPC - INDIAN CONTEXT

- Section 70 of IT Act 2000, CII is defined as: “The computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.”

- “National Critical Information Infrastructure Protection Centre" (NCIIPC) of National Technical Research Organisation (NTRO) as the nodal agency under Section 70A(1) of the Information Technology (Amendment) Act 2008 for taking all measures including associated Research and Development for the protection of CIIs in India.

GAZETTE NOTIFICATION

रजिस्ट्री सं० डी० एल०-33004/99

REGD. NO. D. L.-33004/99

भारत का राजपत्र

The Gazette of India

असाधारण

EXTRAORDINARY

भाग II—खण्ड 3—उप-खण्ड (i)

PART II—Section 3—Sub-section (i)

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

सं. 15] नई दिल्ली, बृहस्पतिवार, जनवरी 16, 2014/पौष 26,1935

No. 15] NEW DELHI, THURSDAY, JANUARY 16, 2014/PAUSHA 26, 1935

संचार और सूचना प्रौद्योगिकी मंत्रालय

(इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग)

अधिसूचना

नई दिल्ली, 16 जनवरी, 2014

सा. का.नि. 18(अ). – केन्द्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 70 क की उपधारा (1), द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र, ब्लाक-III, जेएनयू कैम्पस, नई दिल्ली 110067, जोकि राष्ट्रीय तकनीकी अनुसंधान संगठन के अधीन एक संगठन है, को महत्वपूर्ण सूचना अवसंरचना संरक्षण के क्षेत्र में राष्ट्रीय नोडल अभिकरण अभिहित करती है।

[फा. सं. 9(16)/2004-ई.सी.]

आर.के. गोयल, संयुक्त सचिव

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

(Department of Electronics and Information Technology)

NOTIFICATION

New Delhi, the 16th January, 2014

G.S.R 18(E). – In exercise of the powers conferred by sub-section (1) of Section 70A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby designates the National Critical Information Infrastructure Protection Centre, Block-III, JNU Campus, New Delhi-110067, an organisation under the National Technical Research Organisation, as the national nodal agency in respect of Critical Information Infrastructure Protection.

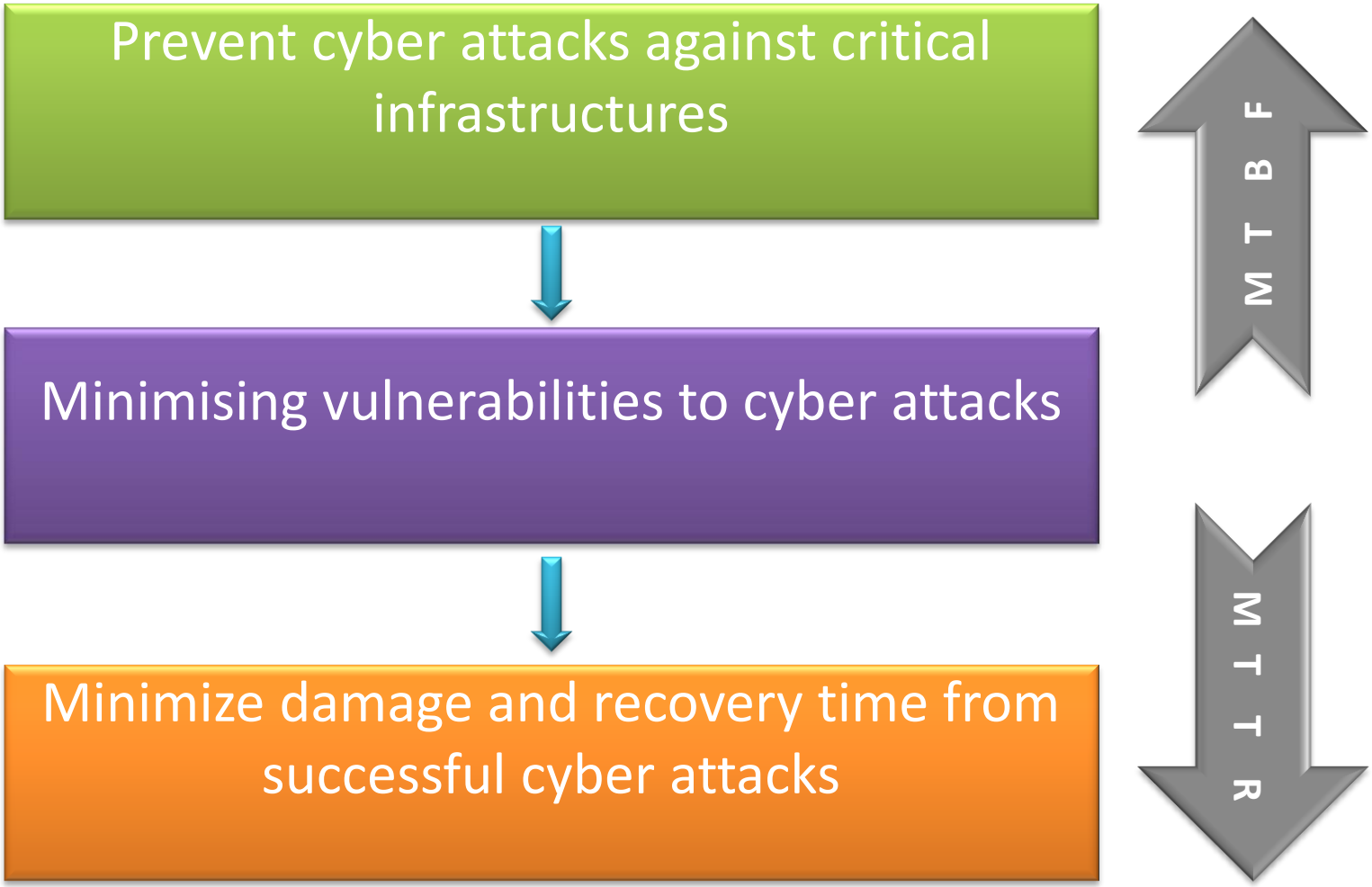
[No. 9(16)/2004-EC]

R.K. GOYAL, Jt. Secy.

NCIIPC - Key Responsibilities

1. National Nodal Agency to protect NCII.
2. Deliver advice to reduce vulnerabilities.
3. Identify all CII elements for notification.
4. Provide strategic leadership and coherent Government response.
5. Coordinate, share, monitor, collect, analyse and forecast threats.
6. Develop plans, adopt standards, share best practices and refine procurement processes.
7. Evolve protection strategies, policies, vulnerability assessment and auditing methodologies and plans for CII.
8. Undertake R&D to create, collaborate and develop technologies for growth of CII protection.
9. Develop training programs for CII protection.
10. Develop cooperation strategies.
11. Issue guidelines, advisories etc. in coordination with CERT-In and other organisations.
12. Exchange knowledge and experiences with CERT-In and other organisations.
13. NCIIPC may call for information and give directions to CII.

Strategic Objectives of NCIIPC



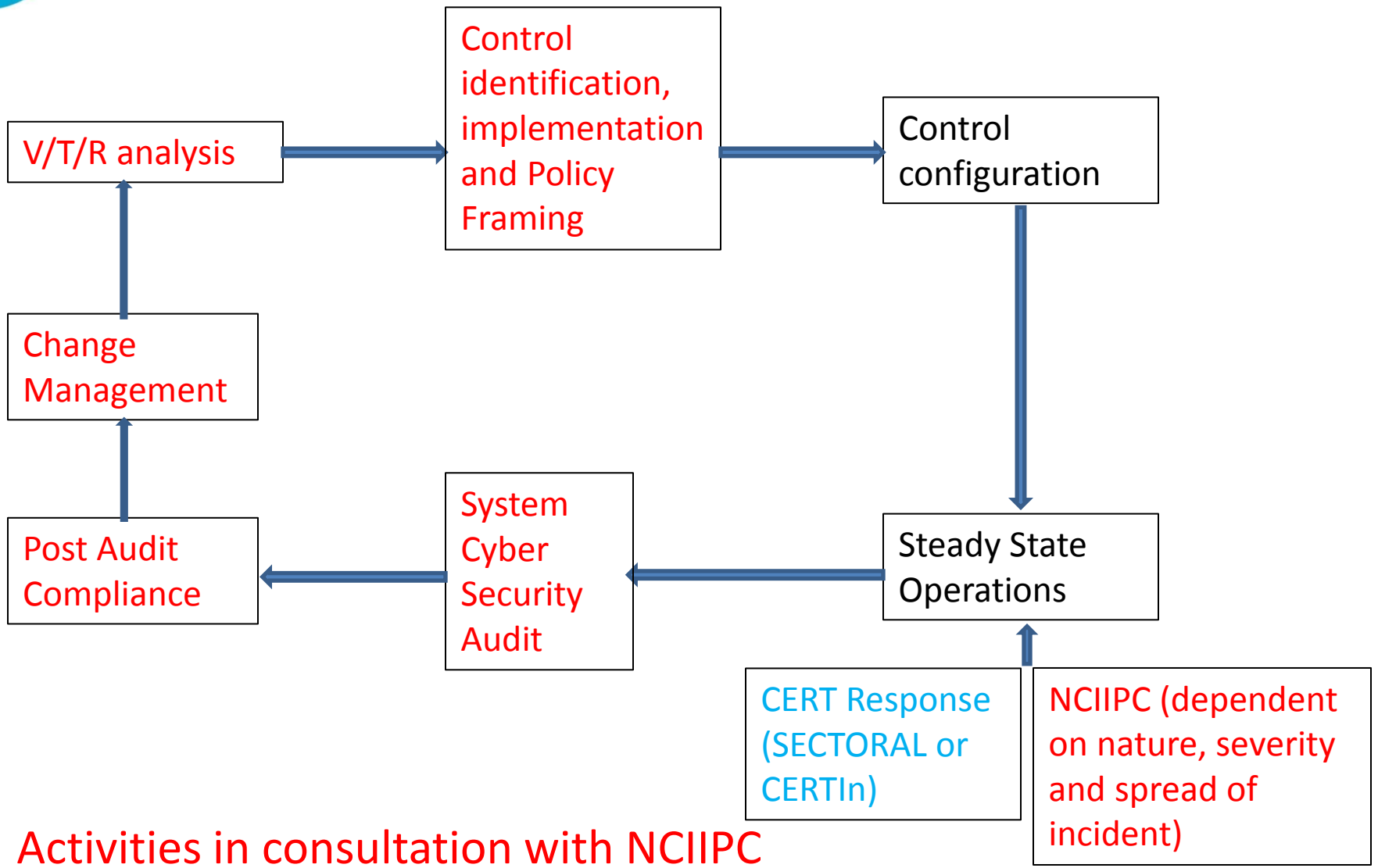
CHALLENGES AHEAD

- IDENTIFYING CII
- RETROMODIFICATION
- IDENTIFYING CII SPECIFIC TRAINING
- ESTABLISHING TRUST AND COHERENCE

WHAT DO WE BRING TO THE TABLE?

1. FOR BOTH EXISTING AS WELL AS NEW / PROPOSED SYSTEMS
   a) Review of the V/T/R and residual risk analysis
   b) Review of Cyber Security Architecture
   c) Alerts, Advisories, RVDP – actionable information
   d) Framing of Cyber Security SLA
   e) Audit Review and compliance

THE MECHANICS



- Activities in consultation with NCIIPC

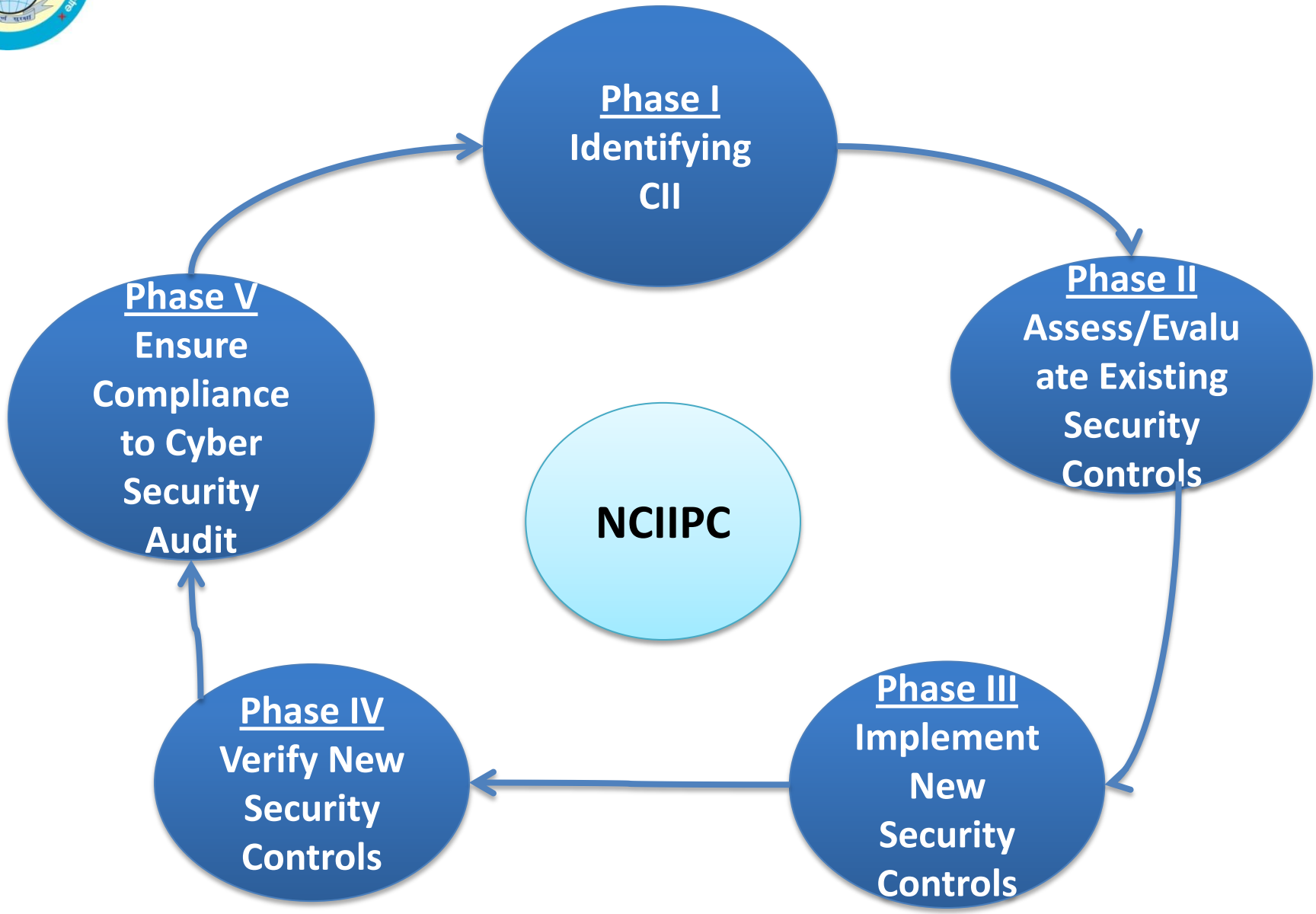
Operational Processes

- A brief request to Center Director NCIIPC for an engagement between the Organisation and NCIIPC
- For existing systems, we revert with a request for V/T/R analysis alongwith cyber security architecture documents
- For new / proposed systems, we provide inputs on the technical (limited to cyber security) aspects of the RFP, if so desired

NCIIPC Framework Documents

- Framework for Protection of Critical Information Infrastructure – Draft
- Evaluating and Enhancing Cyber Security in Critical Information Infrastructure

NCIIPC EF


Phase I
Identifying CII
Phase II
Assess/Evaluate Existing Security Controls
Phase III
Implement New Security Controls
Phase IV
Verify New Security Controls
Phase V
Ensure Compliance to Cyber Security Audit
NCIIPC

NCIIPC : Outreach Program

1. Conferences & Workshops
2. Cyber Security Preparedness Survey
2. Review of Policies/Procurement Tenders/Audit Reports
3. VA/PT
4. KMS
    a. Alerts & Advisories on malicious IPs
    b. CVE Reports
6. Responsible Vulnerability Disclosure Program (RVDP)
7. Partnership with ISACs
8. International Coordination
9. Developed Applications
10. Incidence Response

NCIIPC : Outreach Program

11. Industry Outreach
    a. Av vendors
    b. Training e.g. ISGF, CISOAcademy etc
12. Open to working with industry as part of the ICS / SCADA ecosystem e.g. Honeywell / Intel

"Honeywell will qualify Intel Security's Application Whitelisting and Device Control with its own proprietary cyber security for its Experion® Process Knowledge System, providing a fully vetted and qualified solution designed to increase security without sacrificing reliability. "Protecting our critical infrastructure and the emerging IoT from cyber threats is a priority, and the collaboration of two industry leaders will go a long way toward that goal,"

…Raj Samani, vice president and chief technology officer, Intel Security.

13. In a similar manner, we need to reach out to indigenous OEMs/vendors as well. NCIIPC has begun this action, but we also encourage State partners to identify resources in their states.

The Bottomline

NCIIPC is about Information Assurance and not just cyber security

Contact Details

- Address:

  Block III, Old JNU Campus
  New Delhi 110067

- Telefax:

  +91 9313633455

  1800 11 44 30

- Email:

  helpdesk1.nciipc@nic.in

  helpdesk2.nciipc@nic.in