DNI Special Security Center

Policy & Strategic Planning Division
Core Objectives

- Review, revise, facilitate development of new policies to address mission needs
  - Security policies balance protection and information sharing requirements
  - Comprehensive and ongoing review/transition of security DCIDs to ICDs
- Restructure, clarify and ensure consistency of policies to enhance compliance
  - Security standards to promote reciprocity
  - Policy that provides standard interpretation and application throughout the IC
  - Separate security policy content (“what”) from procedures (“how”)
Policy Outreach

- **National Level Policy**
  - National Security Council (NSC)
  - Policy Coordinating Committees (PCC)
  - Office of Management and Budget (OMB)
  - Information Security Oversight Office (ISOO)
  - National Counterintelligence Executive (NCIX)
  - Committee on National Security Systems (CNSS)
  - Overseas Policy Board (OSPB)
  - Information Sharing Environment Program Manager (ISE PM)

- **Intelligence Community Policy**
  - DDNI/PPR
    - Intelligence Policy Advisory Group (IPAG)
  - ADDNI/FR
    - Foreign Relations Coordinating Committee (FRCC)
  - ADNI CIO
    - IC Information and Technology Governance Board
    - Allied Collaboration Board
  - ADDNI/SEC
    - TK TEM
    - Security Policy Advisory Group (SPAG)

- **Industrial Policy**
  - National Industrial Security Program Policy Advisory Committee (NISPPAC)
  - Industrial Security Working Group (ISWG)

- **DoD Policy**
  - USD (I)
Policy Development Process

Need
(DCID conversion, update or new)

Expert Working Group
or
SSC Lead

SSC Review

Security Policy Advisory Group
(SPAG)

D/SSC Review

ODNI Process

DNI Security Board
(DSB)
(as determined by D/SSC)
UNCLASSIFIED

ICD 700
Protection of National Intelligence

▪ New
  – Overarching Security

▪ Key Elements
  – National Intelligence
  – ADDNI/SEC
  – Sensitive Compartmented Information (SCI)
  – Controlled Access Programs
  – Security Program Oversight
  – Personnel Security
  – Physical/Technical Security
  – Information System Security
  – Uniform Implementation
  – Information Sharing
  – Reciprocity
  – Risk Management
  – “Criteria for Access”
Key Elements cont.
- Insider Threat
- Security Awareness, Training and Education
- Cognizant Security Authority
- Individual Clearance/Access Approval Holders
- SSC
- CSE

Status
- Pending DNI signature

Two ICPGs
- Security Glossary
  - SPAG review
- Governance
  - TBD
Unauthorized Disclosures

- Replaced DCID 6/8
- Key Elements
  - Unauthorized Disclosures and Leaks of Classified Information
  - Reporting Criteria
  - Status Reporting
  - Disposition Reporting
- Status
  - Signed
- No ICPG
- **Replaces DCID 6/2**

- **Key Elements**
  - Threat Assessments
  - Telephone Security
  - Countermeasures
  - NCIX
  - IC Manager for TSCM
  - National Integrated TSCM Committee

- **Major Change**
  - Funding Mechanism
  - National Integrated TSCM Committee

- **Status**
  - DDNI level review

- **One ICPG**
  - TSCM

Key Elements
- SCI
- Intelligence Sources and Methods
- SSO
- Clearance/Access Approval Holders
- Types of Access Approvals
- Courier Operations
- Marking and Packaging
- Document Accountability, Transportation & Destruction
- Dissemination Controls
- Control Centers
- Contractor Program Reviews
- Security Awareness Programs
- Continuing Reporting Requirements (foreign travel, etc.)
- Contractor/Consultant Security
- Industrial & Acquisition Security
- Self Inspections
Key Elements cont.
- Operations Security (OPSEC)
- Risk Management
- Reporting Requirements
- Non-NIP Executive Agent (CSA)
- Non-NIP Agencies & Departments
- Executive Office of the President Elements
- Legislative & Judicial Branch
- State/Local/Tribal Government with Access
- Law Enforcement Access
- Foreign Partners

Major change
- Addition of foreign partner security
- Non-Title 50
- Emergency Disclosure from DCID 6/6
  - Added Secretary of Homeland Security
- “Third Agency Rule” from DCID 6/6
  - Deleted requirement to remove identity of originating agency
  - Removed limitation to disseminate only to Executive Branch of the US Government
- SOICs no longer add “significant threat” countries for foreign travel
  - Only NTIPA & SETL to identify threat to SCI
ICD 703
Protection of SCI and Sources & Methods

| 6/1 | Protection of Sources & Methods |
| 6/1 | Personnel Security               |
| 6/1 | Physical Security                |
| 6/1 | Technical Security               |
| 6/6 | Dissemination and Disclosure Under Emergency Conditions |
| 6/6 | Use By and Dissemination Among Executive Branch Departments/Agencies of the US Government (3rd agency rule waiver) |

1/20P | Hazardous Official Travel        |
1/20P | Hazardous Foreign Travel         |
1/20P | SCI Debrief and Hazardous Travel |
1/20P | Country Annex (previously rescinded) |
6/4  | Reporting Requirements           |

ICPD 703.1
Continuing Reporting

UNCLASSIFIED
### ICD 703

**Protection of SCI and Sources & Methods**

<table>
<thead>
<tr>
<th>Code</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/1</td>
<td>Contractor/Consultant Security</td>
</tr>
<tr>
<td>6/1</td>
<td>SCI Information Services Centers &amp; Security Officials</td>
</tr>
<tr>
<td>6/1</td>
<td>Information Security</td>
</tr>
<tr>
<td>6/1</td>
<td>SCI Security Infractions, Violations, Compromises and Unauthorized Disclosures</td>
</tr>
<tr>
<td>6/1</td>
<td>Program Security Reviews</td>
</tr>
<tr>
<td>6/4</td>
<td>Annex E Standards for SCI Security Awareness Programs</td>
</tr>
<tr>
<td>6/6</td>
<td>Release of Intelligence to Contractors and Consultants</td>
</tr>
</tbody>
</table>

#### Annex E Standards for SCI Security Awareness Programs
- **ICPG 703.2** SCI Management
- **ICPG 703.3** Non-Title 50
  - Legislative Branch Access to SCI
  - Judicial Branch Access to SCI
- **ICPG 703.4** Foreign Partners
  - New: Foreign Partner Security
ICD 703
Protection of SCI and Sources & Methods

<table>
<thead>
<tr>
<th>Area</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use By and Dissemination Among</td>
<td>Use By and Dissemination Among Executive Branch Departments/Agencies of</td>
</tr>
<tr>
<td>Executive Branch Departments/Agencies</td>
<td>the US Government (3rd agency rule waiver)</td>
</tr>
<tr>
<td>of the US Government</td>
<td></td>
</tr>
<tr>
<td>Authorized Control Markings</td>
<td></td>
</tr>
<tr>
<td>Use of Authorized Control Markings</td>
<td></td>
</tr>
<tr>
<td>Reporting Unauthorized Disclosures</td>
<td></td>
</tr>
<tr>
<td>Responsibilities of SOICs</td>
<td></td>
</tr>
<tr>
<td>Annual Report on the Use of Control</td>
<td></td>
</tr>
<tr>
<td>Markings</td>
<td></td>
</tr>
<tr>
<td>Interpretation</td>
<td></td>
</tr>
<tr>
<td>Annex A ORCON</td>
<td></td>
</tr>
<tr>
<td>Annex B IMCON</td>
<td></td>
</tr>
<tr>
<td>NOFORN Criteria</td>
<td></td>
</tr>
</tbody>
</table>

ICPG 703.5 Dissemination Controls (TBD)

ICPG 703.6 Risk Management (TBD)

New Risk Management
Replaces DCID 6/4

Key Elements
- SSBI – SSBI/PR
- Investigative Standards
- Quality Control Guidelines
- Adjudicative Guidelines
- Temporary Eligibility
- Appeals Procedures
- Denial or Revocation of Access
- Reciprocity of Eligibility Determinations
- Personal Reporting Requirements
- SCI Access Approval Database
- Continuing Reliability Monitoring
ICD 704
Personnel Security Standards

- **Major Change**
  - Annex E, *Standards for SCI Security Awareness Programs in the US Intelligence Community*, moved to ICD 703
  - Signal Flags
  - Scattered Castles

- **Issues**
  - 1\textsuperscript{st} and 2\textsuperscript{nd} generation
  - Personnel Security Program Office

- **Five ICPGs**
  - Investigations
  - Adjudications
  - Denials/Revocations
  - Reciprocity
  - Scattered Castles/Signal Flags (May be classified annex)
- Replaces DCID 6/9
- Key Elements
  - SCIF Construction Standards
  - SCIF Administration
  - Locking Devices
  - Accreditation Checklist
  - Accreditation Reciprocity
  - SCIF Database
  - Personnel Access Control
  - Intrusion Detection Systems
  - Telephone Security
  - Portable Electronic Devices
  - Acoustical Control & Sound Masking
  - Emergency Co-Utilization of SCIFs
  - Tactical Operations/Field Training
  - Counterterrorism
  - Laser Toner Cartridges
**Major Changes**

- Separates policy from implementation standards
- Specific forced entry specification
- Single standard (removed “minimum”)
- Wall construction standard specified
- Requires Construction Security Plan
- Sets requirements for workers
- Provides flexibility for covert sites
- Defines the term “Security-in-Depth”
Issues
- Forced Entry Protection
- Alarm Response Time

Ten ICPGs
- Forms
- Facilities inside the US
- Facilities outside the US
- Tactical SCIFs
- PEDs
- Acoustic Control
- Intrusion Detection
- Personnel Access Control
- Telecommunications
- SCIF Administration
ICD 705
Physical/Technical Security Standards

6/9 Policy and Concept

6/9 Annex A SCIF Accreditation Checklist

6/9 Construction Specifications

6/9 Physical Security Construction Policy

6/9 Annex C Tactical Operations

6/9 Annex D Electronic Equipment/Toner

6/9 Annex E Acoustical Control

6/9 Annex B Intrusion Detection Systems

6/9 Annex F Personnel Access Controls

6/9 Annex G Telephone Security

6/9 General Administrative

ICPD 705.1 Forms

ICPD 705.2 Domestic SCIF

ICPD 705.3 Overseas SCIF

ICPD 705.4 Tactical SCIF

ICPD 705.5 PEDs

ICPD 705.6 Acoustical Control

ICPD 705.7 Intrusion Detection

ICPD 705.8 Personnel Access Controls

ICPD 705.9 Telecommunications

ICPD 705.10 SCIF Administration
Replaces DCID 6/11

Key Elements
- Controlled Access Programs
- Restricted Collateral Information
- CAPOC
- SRG
- CAPCO
- CMIWG
- Classification Guidance
- Virtual Classification Manual (Annex)
- Register

Major Change
- Potential SRG scope change

One ICPG
- Controlled Access Program Governance/Management
- New
  - Define CSE roles and responsibilities

- Key Elements
  - Construction Security Review Board (CSRB)
  - References to:
    - TSCM responsibilities
    - COOP/COG responsibilities

- One ICPG
  - CSRB
New
- Standardize IC TEMPEST activities
- Specific guidance and interpretation of national standard

Key Elements
- TEMPEST
- “Inspectable” Space
- Red/Black Separation Uniformity
- Reciprocity
- RFID
- Risk Management
## DCID Conversion

<table>
<thead>
<tr>
<th>DCID</th>
<th>TOPIC</th>
<th>ICD</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/20P</td>
<td>Hazardous Official Travel</td>
<td>703.1</td>
<td></td>
</tr>
<tr>
<td>1/20P</td>
<td>Hazardous Foreign Travel</td>
<td>703.1</td>
<td></td>
</tr>
<tr>
<td>1/20P</td>
<td>SCI Debrief and Hazardous Travel</td>
<td>703.1</td>
<td></td>
</tr>
<tr>
<td>1/20P</td>
<td>Country Annex (previously rescinded)</td>
<td>703.1</td>
<td>Refer to Department of State’s Security Environment Threat List (SETL) and NCIX National Threat Identification and Prioritization Assessment (NTIPA)</td>
</tr>
<tr>
<td>6/1</td>
<td>Protection of Sources &amp; Methods</td>
<td>703</td>
<td></td>
</tr>
<tr>
<td>6/1</td>
<td>Personnel Security</td>
<td>703</td>
<td>Items covered by ICD 704 will not be repeated</td>
</tr>
<tr>
<td>6/1</td>
<td>Physical Security</td>
<td>703</td>
<td>Items covered by ICD 705 will not be repeated</td>
</tr>
<tr>
<td>6/1</td>
<td>Technical Security</td>
<td>703</td>
<td>Items covered by ICD 702 will not be repeated. (nothing in this section is covered by ICD 705)</td>
</tr>
<tr>
<td>6/1</td>
<td>Contractor/Consultant Security</td>
<td>703.2</td>
<td></td>
</tr>
<tr>
<td>6/1</td>
<td>SCI Information Services Centers &amp; Security Officials</td>
<td>703.2</td>
<td></td>
</tr>
<tr>
<td>6/1</td>
<td>Information Security</td>
<td>703.2</td>
<td></td>
</tr>
<tr>
<td>6/1</td>
<td>SCI Security Infractions, Violations, Compromises and Unauthorized Disclosures</td>
<td>703.2</td>
<td>Items covered by ICD 701 will not be repeated</td>
</tr>
<tr>
<td>6/1</td>
<td>Program Security Reviews</td>
<td>703.2</td>
<td></td>
</tr>
<tr>
<td>6/1</td>
<td>Legislative Branch Access to SCI</td>
<td>703.3</td>
<td></td>
</tr>
<tr>
<td>DCID</td>
<td>TOPIC</td>
<td>ICD</td>
<td>Comment</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------------</td>
<td>-------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>6/1</td>
<td>Judicial Branch Access to SCI</td>
<td>703.3</td>
<td></td>
</tr>
<tr>
<td>6/2</td>
<td>TSCM</td>
<td>702</td>
<td></td>
</tr>
<tr>
<td>6/3</td>
<td>Protecting SCI within Information Systems</td>
<td>500 Series</td>
<td>All topics and appendices</td>
</tr>
<tr>
<td>6/4</td>
<td>Reporting Requirements</td>
<td>703.1</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Annex E Standards for SCI Security Awareness Programs</td>
<td>703.2</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Personnel Security Standards</td>
<td>704</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Exceptions to Personnel Security Standards</td>
<td>704</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Investigative Requirements and Standards</td>
<td>704.1</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Temporary Eligibility for Access to SCI</td>
<td>704.1</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Annex A Investigative Standards</td>
<td>704.1</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Annex B Quality Control Guidelines for the SSBI</td>
<td>704.1</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Annex C Adjudication Guidelines</td>
<td>704.2</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Annex D Appeals Procedures: Denial or Revocation</td>
<td>704.3</td>
<td></td>
</tr>
<tr>
<td>6/4</td>
<td>Annex F Reciprocity</td>
<td>704.4</td>
<td></td>
</tr>
</tbody>
</table>
## DCID Conversion

<table>
<thead>
<tr>
<th>DCID</th>
<th>TOPIC</th>
<th>ICD</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/5</td>
<td>SAMI</td>
<td></td>
<td>Rescind</td>
</tr>
<tr>
<td>6/6</td>
<td>Dissemination and Disclosure Under Emergency Conditions</td>
<td>703</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Release of Intelligence to Contractors and Consultants</td>
<td>703.2</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Use By and Dissemination Among Executive Branch Departments/Agencies of the US Government (3rd agency rule waiver)</td>
<td>703.5</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Authorized Control Markings</td>
<td>703.5</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Use of Authorized Control Markings</td>
<td>703.5</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Reporting Unauthorized Disclosures</td>
<td>703.5</td>
<td>703.7 will reference ICD 701 - this relates to UDAs as a result of not handling per the control marking.</td>
</tr>
<tr>
<td>6/6</td>
<td>Responsibilities of SOICs</td>
<td>703.5</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Annual Report on the Use of Control Markings</td>
<td>703.5</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Interpretation</td>
<td>703.5</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Annex A ORCON</td>
<td>703.5</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Annex B IMCON</td>
<td>703.5</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Release to Foreign Governments, International Organizations, and Coalition Partners</td>
<td>400 Series</td>
<td></td>
</tr>
<tr>
<td>6/6</td>
<td>Dissemination to Non-Governmental Foreign Nationals or Foreign Contractors</td>
<td>400 Series</td>
<td></td>
</tr>
<tr>
<td>DCID</td>
<td>TOPIC</td>
<td>ICD</td>
<td>Comment</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------------------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>6/6</td>
<td>Obsolete Restrictions and Control Markings</td>
<td></td>
<td>Rescind</td>
</tr>
<tr>
<td>6/7</td>
<td>Intelligence Disclosure Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/8</td>
<td>Unauthorized Disclosures, Security Violations, and Other Compromises of Intelligence Information</td>
<td>701</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>Policy and Concept</td>
<td>705</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>Annex A SCIF Accreditation Checklist</td>
<td>705.1</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>General Administrative</td>
<td>705.10</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>Annex C Tactical Operations</td>
<td>705.4</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>Annex D Electronic Equipment/Toner</td>
<td>705.5</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>Annex E Acoustical Control</td>
<td>705.6</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>Annex F Personnel Access Controls</td>
<td>705.8</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>Annex G Telephone Security</td>
<td>705.9</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>Construction Specifications</td>
<td>705.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>705.3</td>
<td></td>
</tr>
<tr>
<td>6/9</td>
<td>Physical Security Construction Policy</td>
<td>705.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>705.3</td>
<td></td>
</tr>
<tr>
<td>6/11</td>
<td>CAPOC</td>
<td>706</td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>Foreign Partner Security</td>
<td>703.4</td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>Risk Management</td>
<td>703.6</td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>Scattered Castles</td>
<td>704.5</td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>Center for Security Evaluation</td>
<td>707</td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>Tempest</td>
<td>708</td>
<td></td>
</tr>
</tbody>
</table>