Topic 1. Establishing a Secure and Trustworthy ICT Environment

1.2 Secure and Trusted e-Government Services

Research, Development and Evaluation Commission, Executive Yuan

August 18th, 2009

Outline

1. Vision
2. Current Status
3. Global Cybersecurity Trends
4. Strategies
5. Action Plans
6. Issues

1. Vision

e-Government Program(2008-2011)

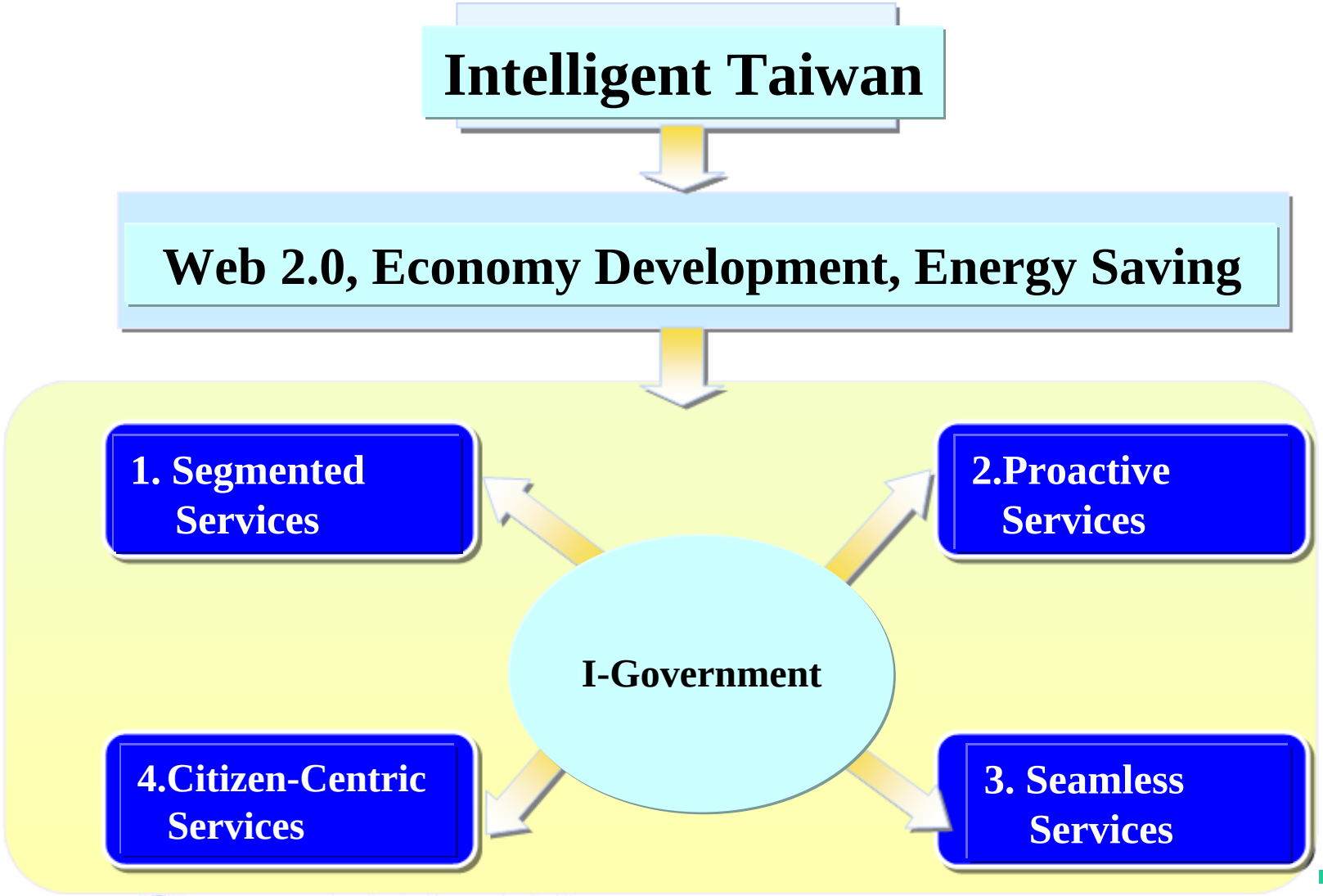
Vision：
Enhance public values and
establish a trusted and connected society

3 Main Goals

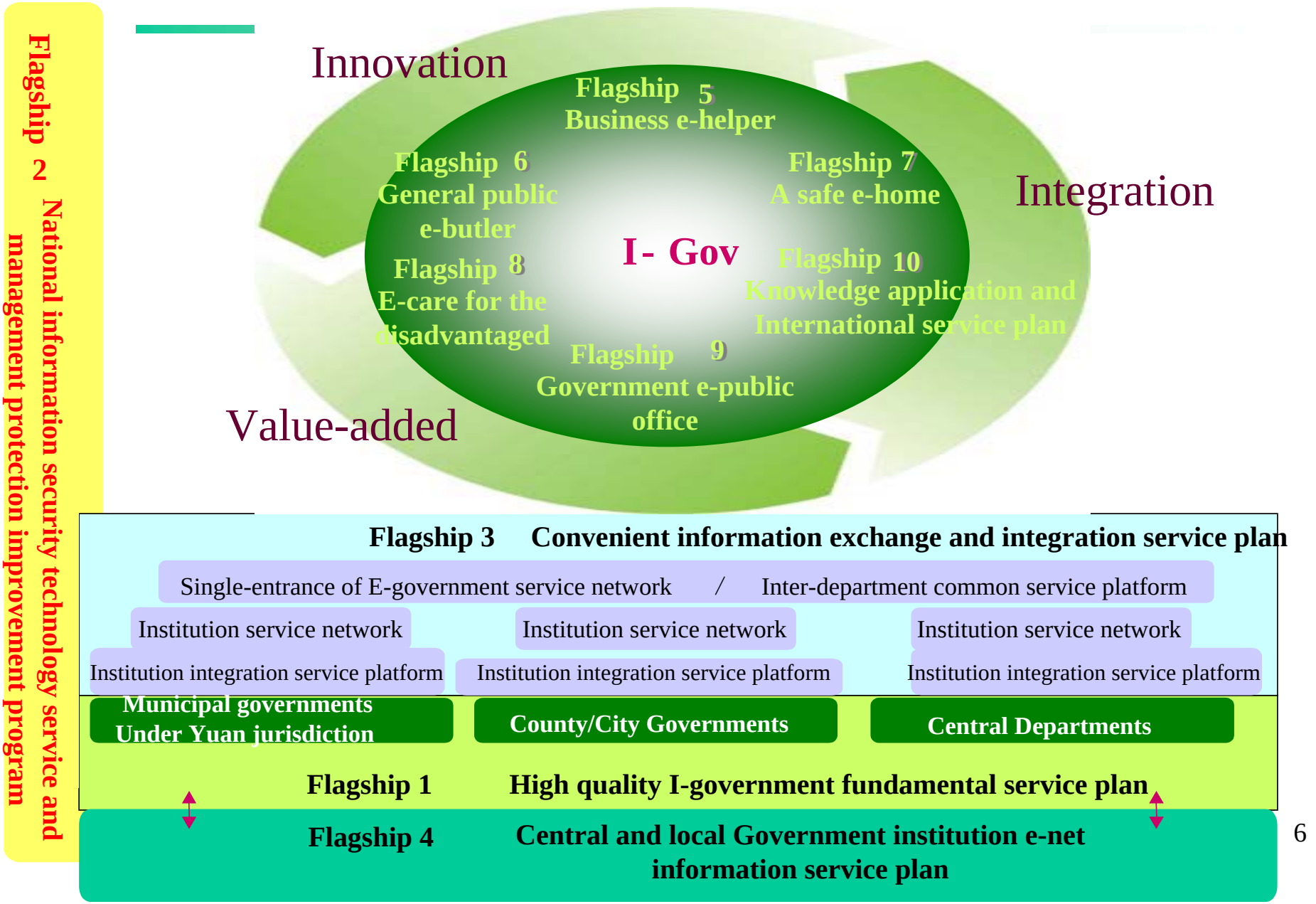
1. **Provide Multi-Channel Services; Enrich Quality Life-Style**
2. **Prevail Informative Services; Enhance Social Care**
3. **Strengthen Citizen Interaction; Broaden e-Participation**

5 Strategies	Strategy 1. IT transformation for efficient resources utilization
	Strategy 2. Integration of government service workflows
	Strategy 3. Legislation for advanced e-government
	Strategy 4. Provision of on-demand services to citizens
	Strategy 5. Enhanced e-government marketing and greater citizen satisfaction

Major Focus of the e-Government Program(2008-2011)

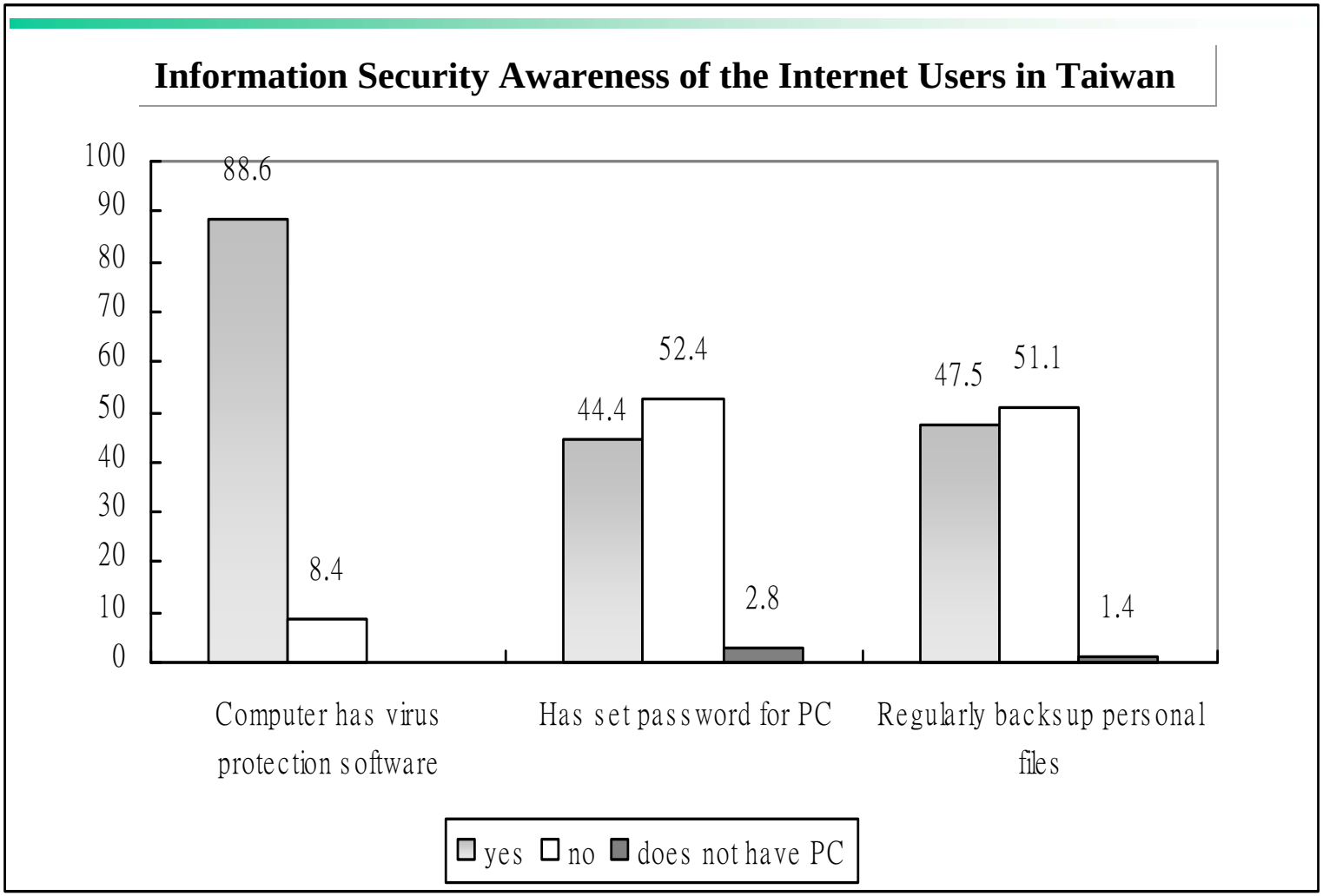


Flagship Projects



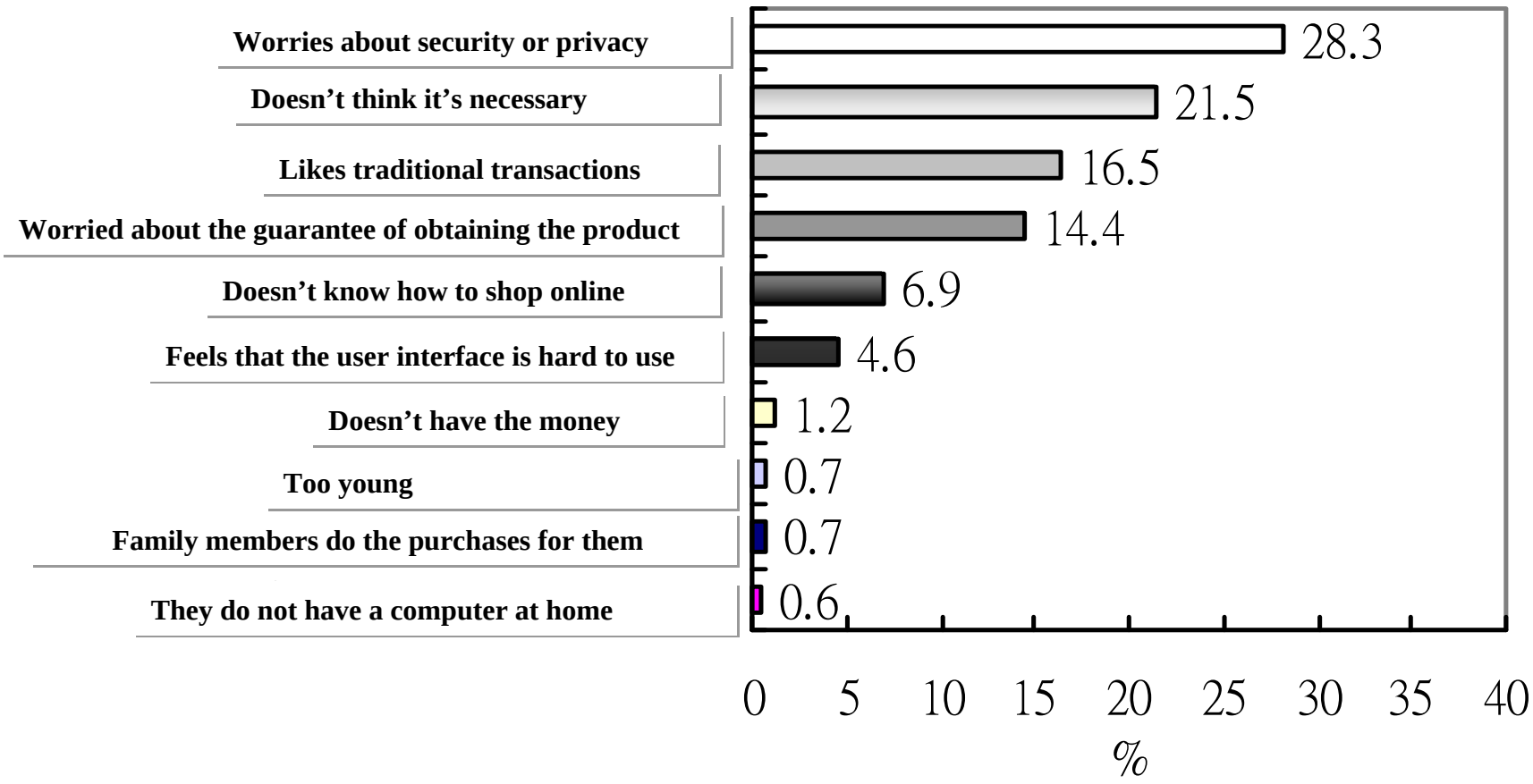
2. Current Status

Information Security Awareness of Internet Users in Taiwan



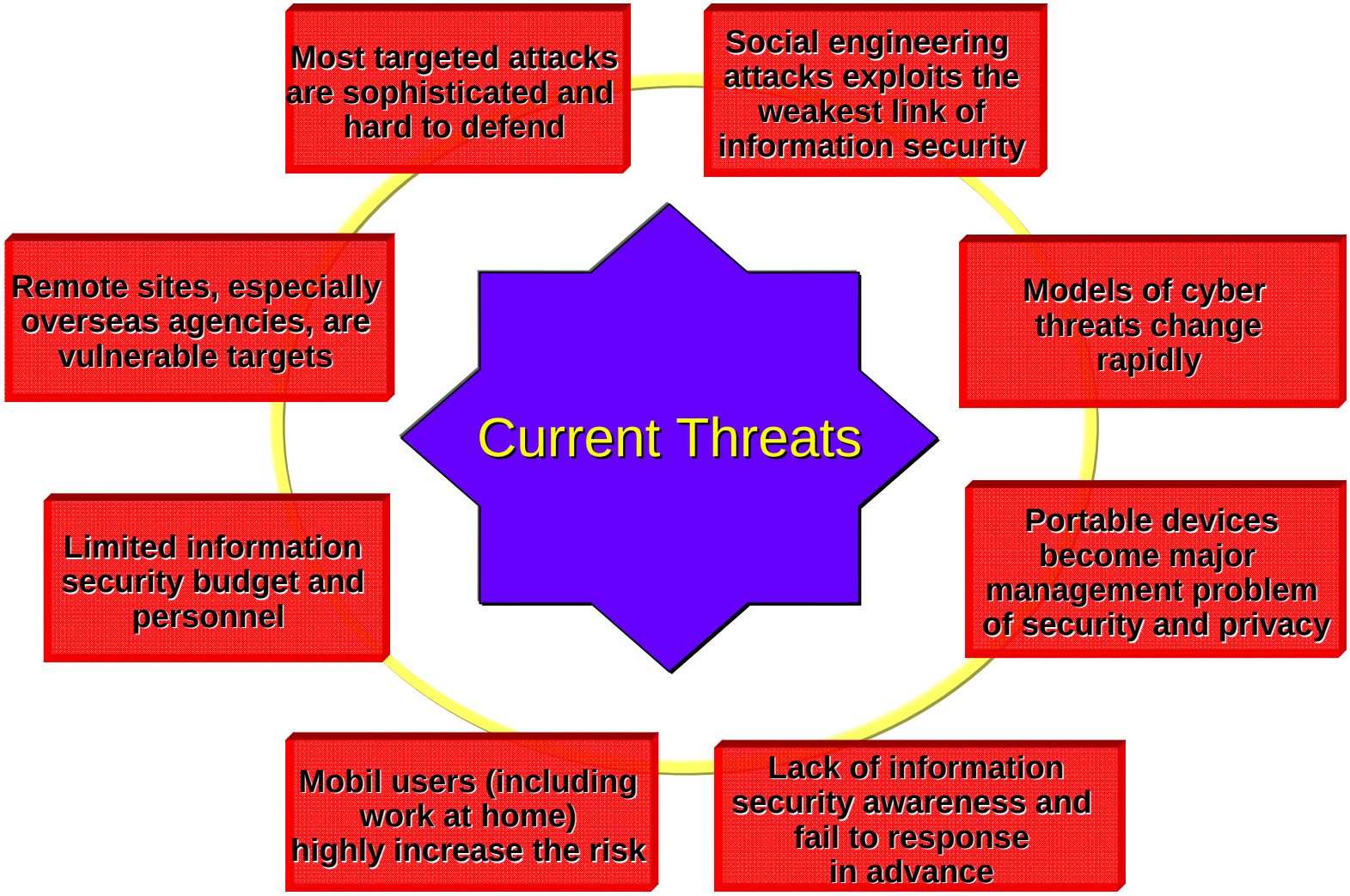
Information source：2008 digital difference report, RDEC, October 2008

Why Internet Users Have Never Participated in Online Transactions



Information source：2008 digital difference report, RDEC, October 2008

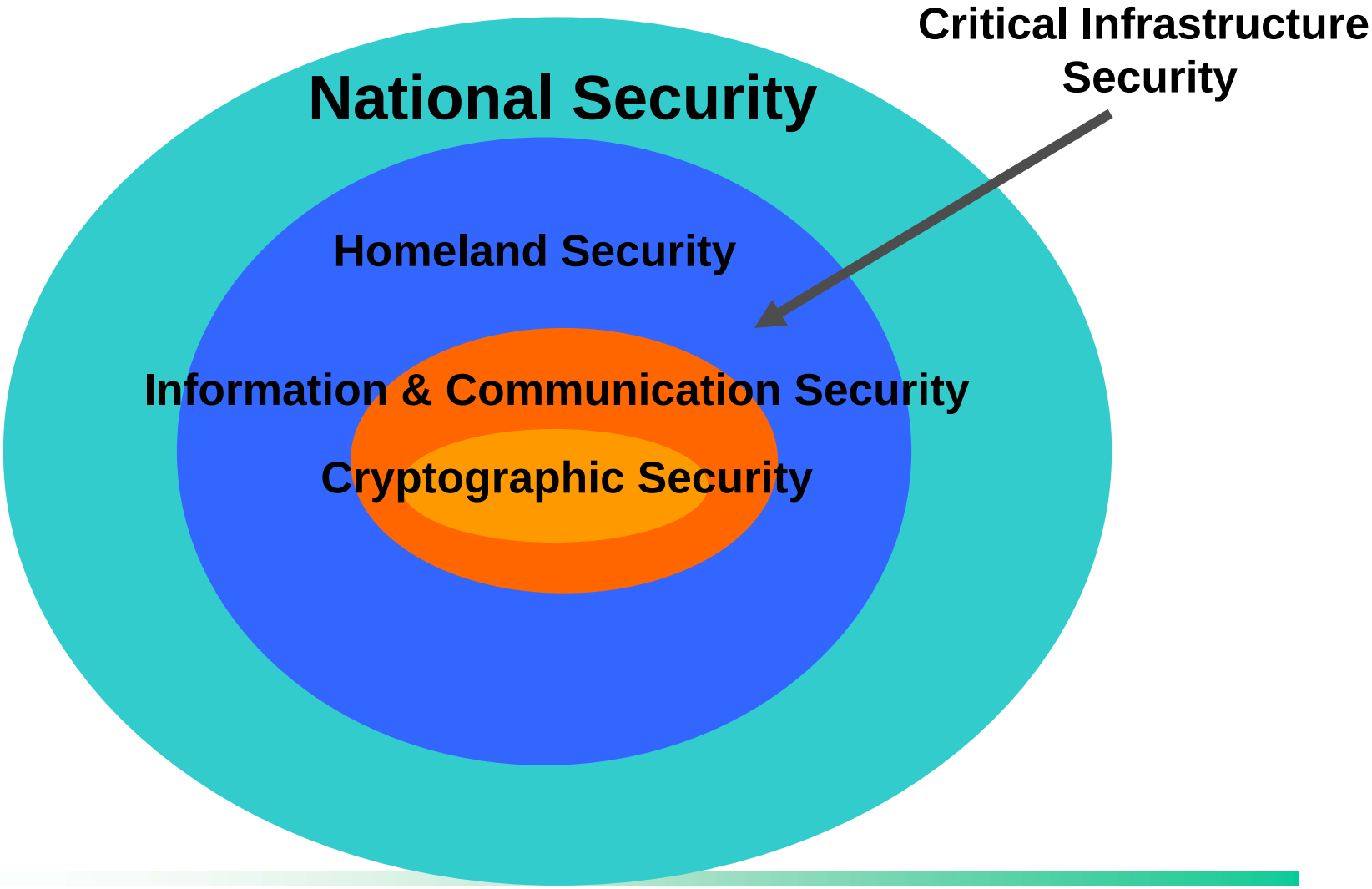
Current Information Security Threats



Government Information Security Issues

- **External Threats**
  - ✓ Targeted attacks launched by organized hacker groups
  - ✓ Attacks toward specific targets or divisions
  - ✓ Rapidly changing attack vectors and models
- **Internal Threats**
  - ✓ Limited information security personnel
  - ✓ Unwillingness to report information security incidents
  - ✓ ICT outsourcing and quality management problems
  - ✓ IT operation outsourcing and its derived information security problems
  - ✓ Lack of information security awareness
  - ✓ Message exchange and communication channel across different functional agencies has not yet been well-established

Information Security is a National Security Priority

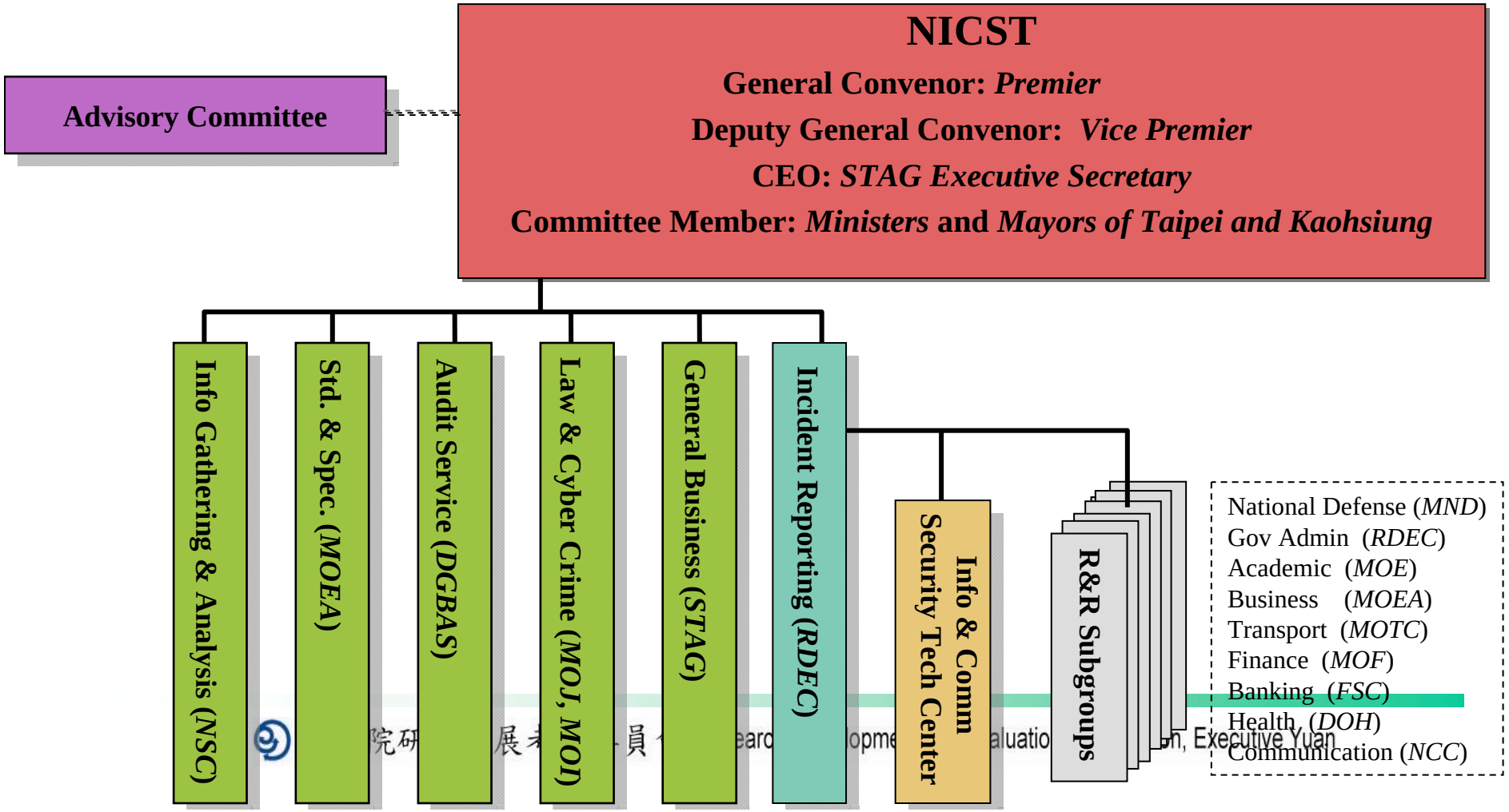


National Information & Communication Security Taskforce

In order to promote information security policy,

the Executive Yuan established the NICST in January 2001.

Starting in 2005, the RDEC is in charge of Incident reporting



Incident Reporting Working Group

NICST

ICST

RDEC
(Incident reporting working group)

Establish a information security report and warning system

Provide 24/7 Surveillance service to sensitive institutions

Reporting, Warning, Responding, Training

- Handle information security incidents and emergency response
- Provide pre-incident security protection
- Provide advanced warning and responding during the incident
- Provide post-incident recovery and forensics
- Provide information security training and promotion

Assist the government in maintaining Information security

about 7,500 government agencies, and 15,000 information security contacts

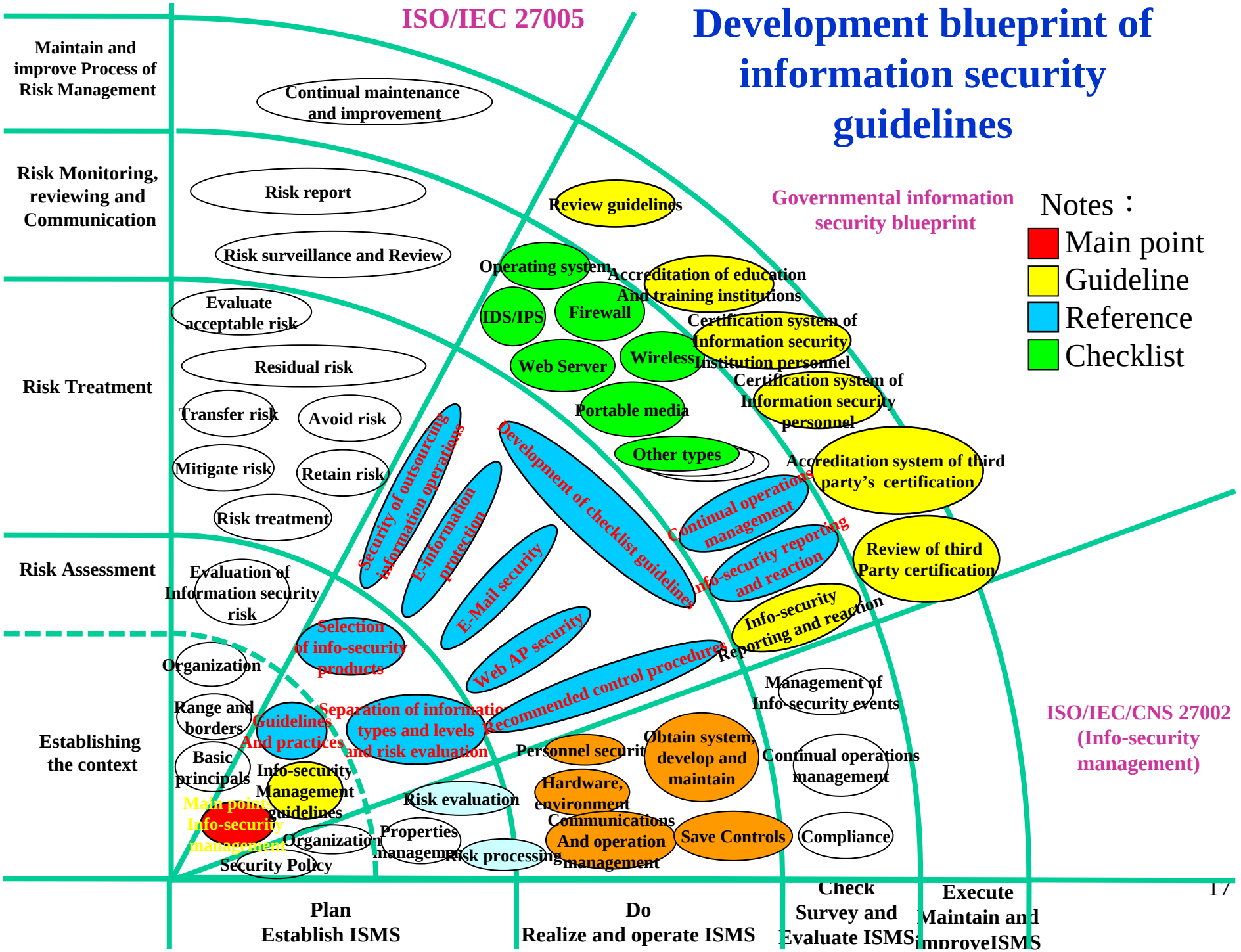
Information Security Incidents Influence Levels

Evaluation Type / Influence Level		Confidentiality	Integrity	Availability
Not as Serious ↕ Serious	*Level 1*	The leak of non-core affair information	The modification of non-core systems or information	The operation of non-core systems are effected or temporarily stopped
	Level 2	The leak of core affair information which is not confidential or sensitive	The slight modification of core systems or information	The operation of core systems are effected or become less efficient but were able to return to normal within an acceptable amount of time
	Level 3	The leak of core affair information which is confidential or sensitive	The major modification of core systems or information	The operation of core systems are stopped and are not able to return to normal within an acceptable amount of time
	Level 4	The leak of national security related confidential information	The major modification of important national infrastructure systems or information	The operation of important national infrastructure is effected or stopped and is not able to return to normal within an acceptable amount of time

Improvement of E-mail Security Awareness

Year / Drill Result	2007	2008
Percentage of personnel opening test e-mails	24.17%	22.16%
Percentage of personnel click links on test e-mails	16.29%	12.82%
Notification before Drill	Yes	No

Note：Objects of the Drill were government agencies and local governments


ISO/IEC 27005
Development blueprint of information security guidelines
Maintain and improve Process of Risk Management
Continual maintenance and improvement
Risk Monitoring, reviewing and Communication
Risk report
Risk surveillance and Review
Risk Treatment
Evaluate acceptable risk
Residual risk
Transfer risk
Avoid risk
Mitigate risk
Retain risk
Risk treatment
Risk Assessment
Evaluation of Information security risk
Establishing the context
Organization
Range and borders
Basic principals
Main point
Info-security management
Security Policy
Organization
Info-security Management guidelines
Guidelines And practices
Selection of info-security products
Separation of information types and levels and risk evaluation
Properties management
Risk evaluation
Risk processing
Review guidelines
Governmental information security blueprint
Operating system
IDS/IPS
Firewall
Web Server
Wireless
Portable media
Other types
Security of outsourcing information operations
E-information protection
E-Mail security
Web AP security
Development of checklist guidelines
Recommended control procedures
Notes：
Main point
Guideline
Reference
Checklist
Accreditation of education And training institutions
Certification system of information security Institution personnel
Certification system of Information security personnel
Accreditation system of third party's certification
Review of third Party certification
Continual operations management
Info-security reporting and reaction
Info-security Reporting and reaction
Management of Info-security events
Continual operations management
Obtain system, develop and maintain
Personnel security
Hardware, environment
Communications And operation management
Save Controls
Compliance
ISO/IEC/CNS 27002 (Info-security management)
Plan
Establish ISMS
Do
Realize and operate ISMS
Check
Survey and Evaluate ISMS
Execute
Maintain and improveISMS

3. Global Cybersecurity Trends

Trends of International Information Security

- The first cyber warfare taken place in Estonia shows the importance of Internet security to overall national security
- President Obama of the United States of America will appoint an Internet security officer to strengthen information security of US government
- Financial fraud loss due to personal and privacy information thefts is becoming more and more frequent
- Information security risks of critical infrastructure are increasing
- Organized hacker groups constantly conduct government information espionage
- Zero-day attack vulnerabilities make defense-in-depth ineffective

Changing of National Security Strategy – Preparing for a New Threat

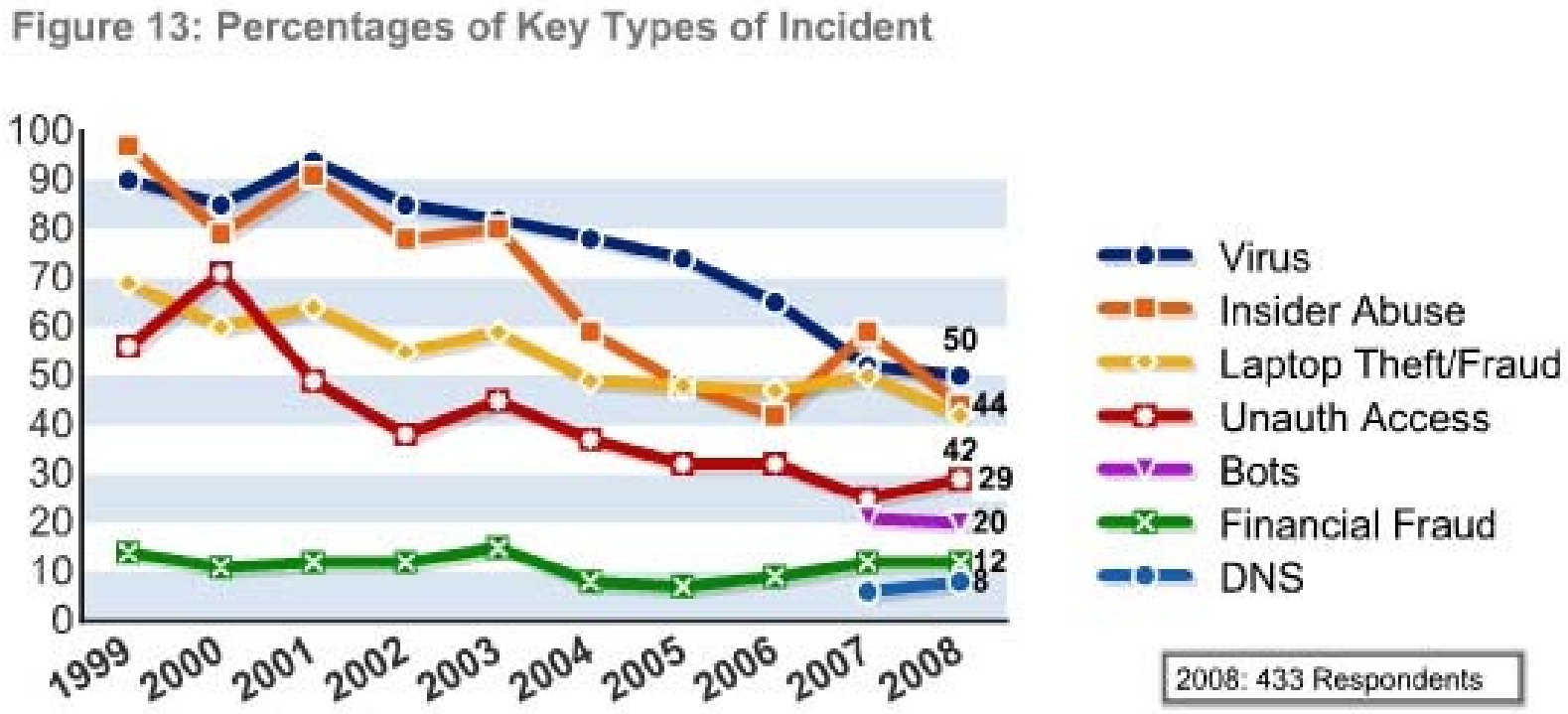
- **In June of 2008 France announced a new national defense and security white paper**
  - ✓ **France adjusted its national security strategy for the next 15 years, returning to NATO, and establishing strategic cooperation with its allies**
  - ✓ **France's proposed main adjustments in strategy include:**
    - ✓ **The threat of terrorism**
    - ✓ **The threat of Internet attacks**
    - ✓ **The threat of the rise of Asia**
    - ✓ **Energy and environmental security threats**

Obama's Internet Security Report

- **The Center for Strategic and International Studies (CSIS) gave an Internet security report to president Obama on December 8th 2008 which contained the following three discoveries**
  - ✓ **Cybersecurity is now a major national security problem for the United States**
  - ✓ **Decisions and actions must respect privacy and civil liberties**
  - ✓ **Only a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will make us more secure**

CSI/FBI 2008 Computer Crimes and Information Security Investigation

➢ **Percentages of key types of incident between 1999~2008**



CSI/FBI 2008 The 13th Computer Crime and Security Survey

Info source：*Computer Security Institute*

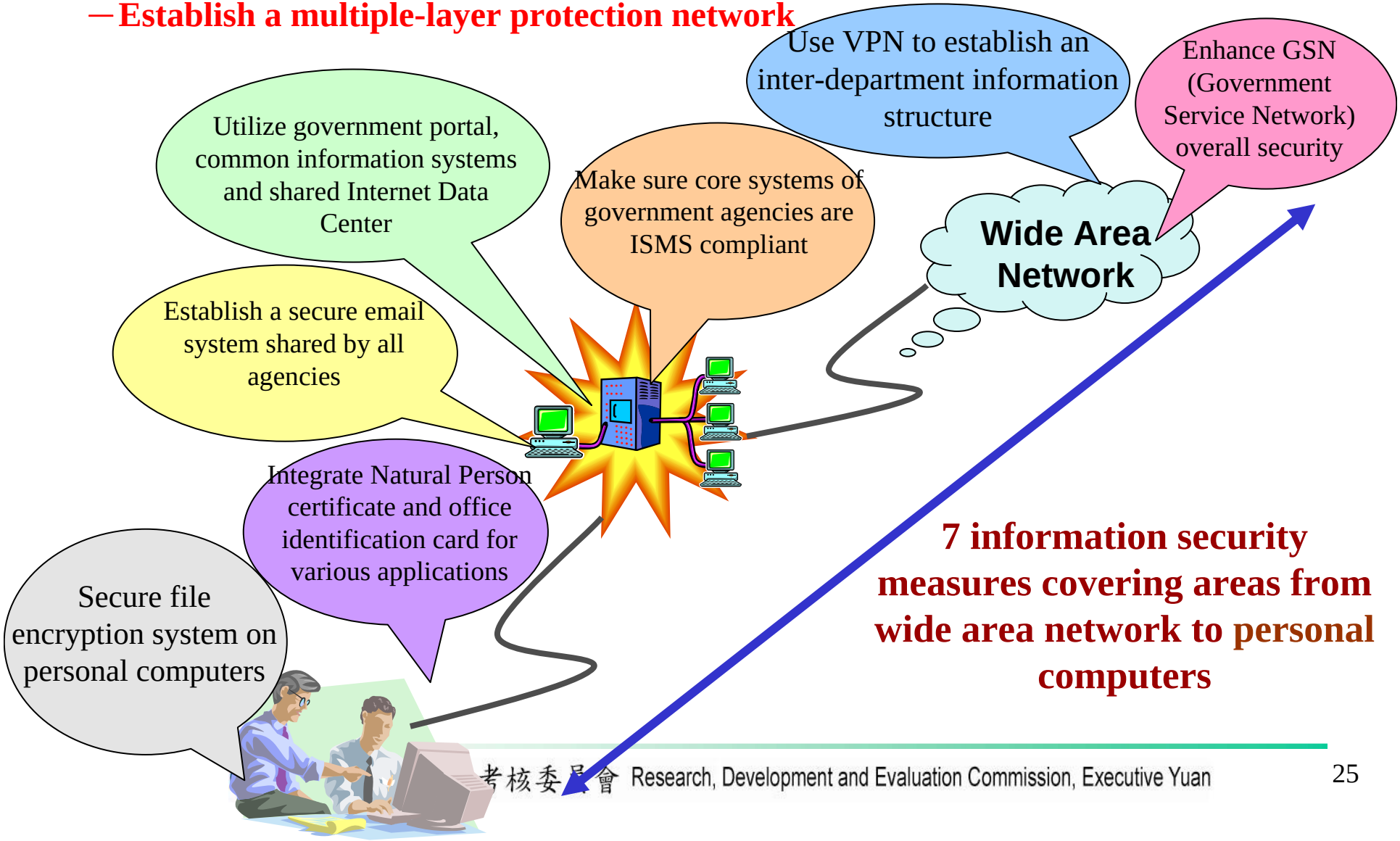
4. Strategies

Government Information Security Strategies

- **The work of governmental information security needs to be maintained comprehensively and continuously**
- **The 3 "E"s government information security strategies**
  - ✓ **Engineering：utilize firewall, digital certificates and data encryption etc. to establish front-line of defense**
  - ✓ **Enforcement：implement information security management policy, urgent incident response mechanism, internal and external computer audit, information security standards and guidelines, product and system quality inspection mechanism**
  - ✓ **Education：enhance information security awareness, campaign personnel training and ethics of Internet usage**

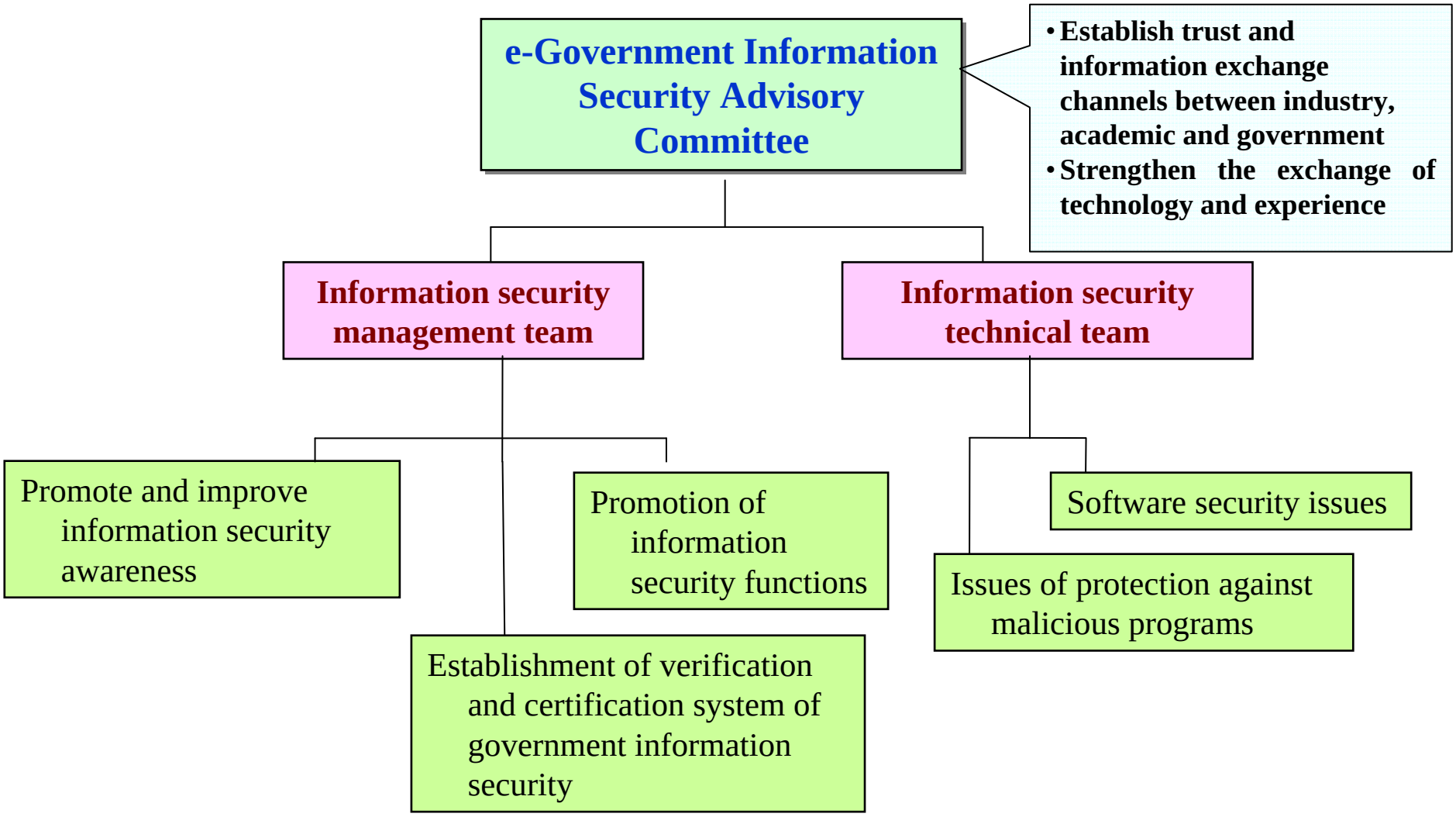
Strategy 1 – Engineering

- **Promote the reform of government information services**
  – Establish a multiple-layer protection network



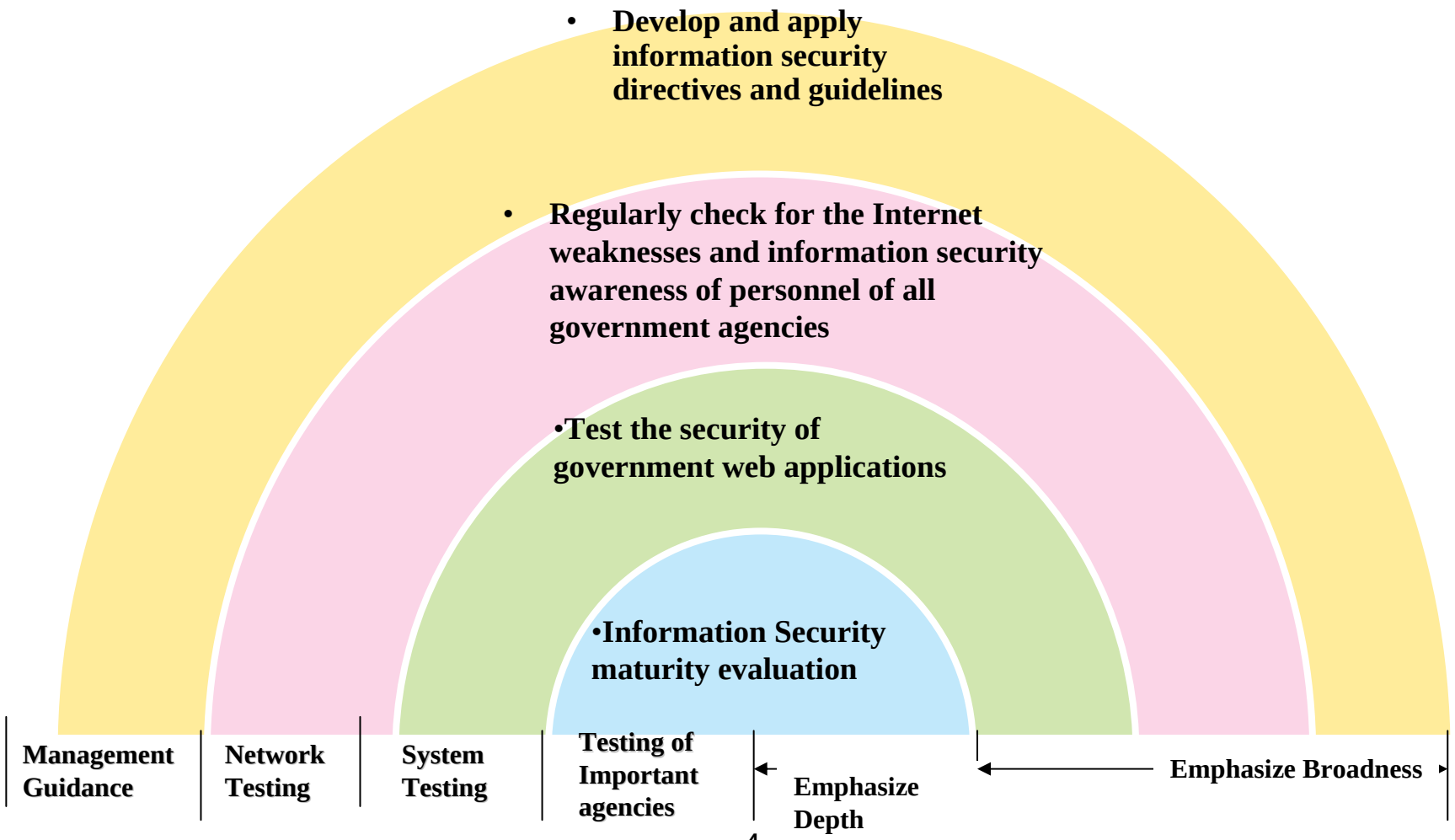
7 information security measures covering areas from wide area network to personal computers

e-Government Information Security Advisory Committee



Strategy 2 – Enforcement

➢ **Improvement of information security management & system security**

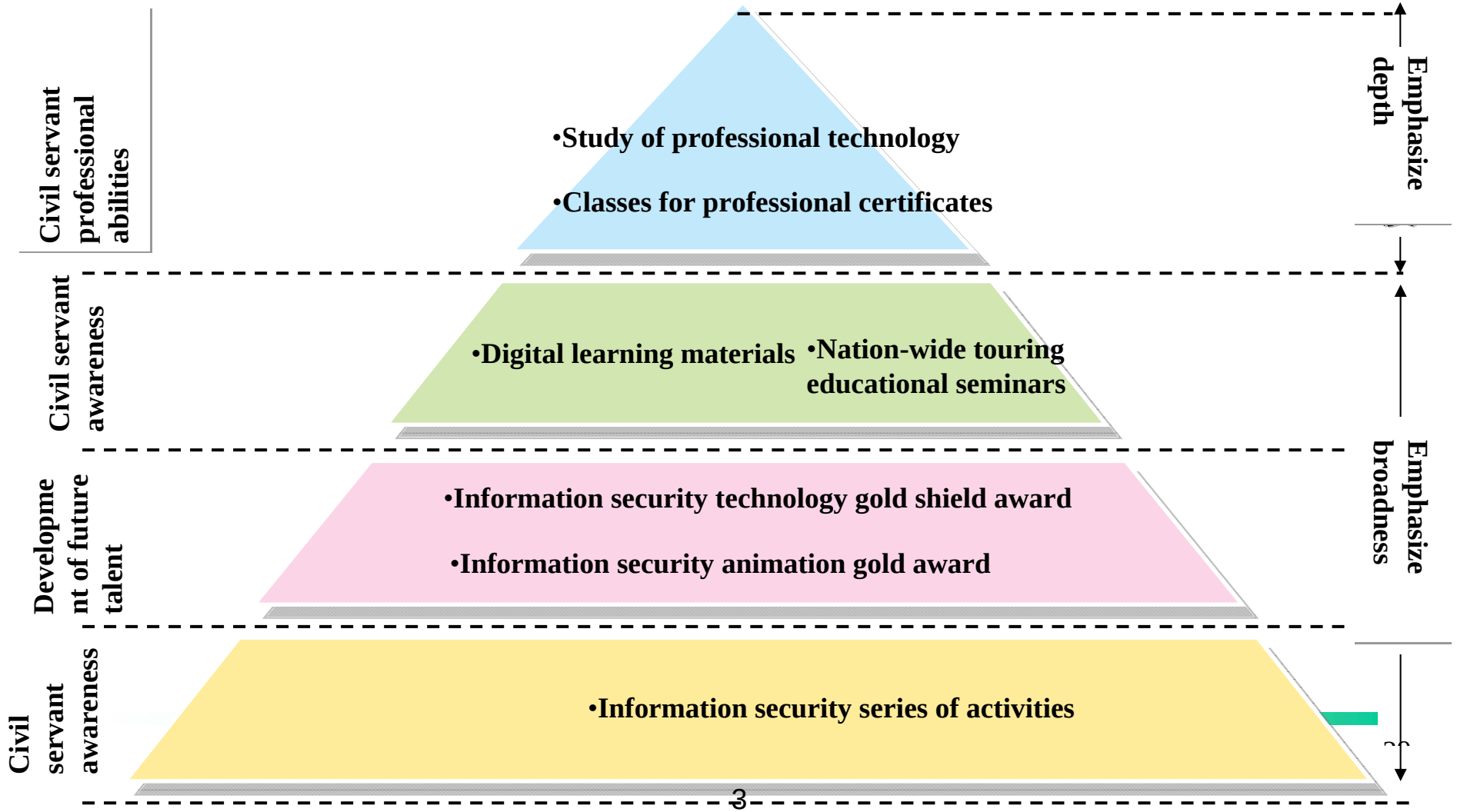


Strategy 2－Important Actions

- Establish an information security accreditation and certification system for government agencies
- Promote information security management systems (ISMS) certification for critical agencies
- Increase the proportion of information security spending within government's ICT budget by 1% every year, will reach 10% by 2012
- Improve the quality of Web applications by improving the ability of testing and patching

Strategy 3－Education

➢ **Improve information security knowledge and competence**



Promote Information Security Training and Evaluation System for Government Officials

Purpose of the plan

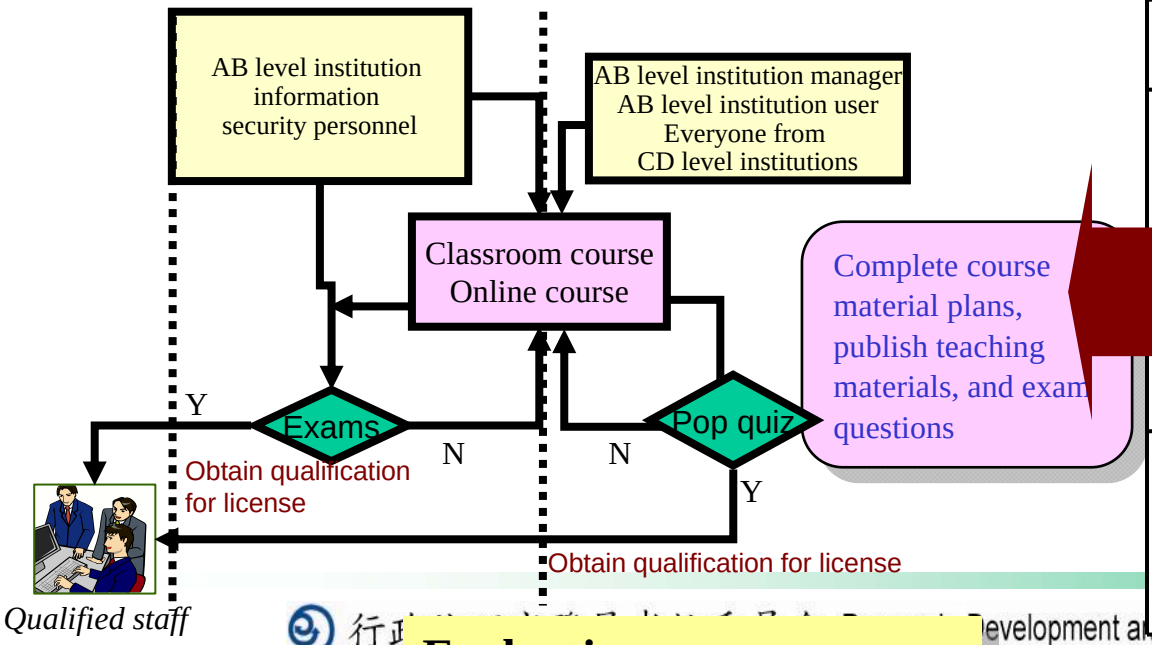
Planning for the information security and skills needed for civil servants to carry out the operations of government institutions

Personnel types	Needed abilities
Normal Manager	Basic information security concepts and related guidelines
Information personnel	Information security management, technology and related knowledge
Normal user	Basic knowledge and related guidelines of information security management topics
Information security personnel	Information security management, technology, and examination knowledge

Course Design

Course design principals are based on the needs of daily information security work of civil servants

Lesson types
Basic information security
Information security management
Information security technology
Other



Complete course material plans, publish teaching materials, and exam questions

Evaluation process

Types	Required courses
Normal manager	➢*B09* Institution information security guidelines ➢*B12* E-mail security (reference guide)
Information personnel	➢*B01* Information security management systems ➢*B07* Government information operations outsourcing security (reference guide) ➢*B10* Digital information protection (reference guide) ➢*B12* E-mail security (reference guide) ➢*C12 Web* application program security (reference guide)
Normal users	➢*B01* Information security management system ➢*B09* Institutional IT guidelines ➢*B10* Digital information protection (reference guide) ➢*B12* E-mail security (reference guide)
Information security personnel	➢*B01* Information security management systems ➢*B03* Information systems risk evaluation(reference guide) ➢*B06* Information security examination ➢*B07* Government information operations outsourcing security(reference guide) ➢*C12 Web* application program security (reference guide)

Training Lessons

The First Information Security Week in December 2008

- International forums
- Information security day
- Information security awards
- Information security e-learning
- ICST website treasure hunt
- The truth about internet security

5. Action Plans

National Information Security Development Plan (2009-2012)

- **e-Government related action plans**
  - ✓ **Action Plan 1**：Improve incident report effectiveness
  - ✓ **Action Plan 2**：Establish an information security event management and response procedure
  - ✓ **Action Plan 5**：Develop and maintain information security operation directives and guidelines for government agencies
  - ✓ **Action Plan 8**：Strengthen e-government information security and implement the information protection of business data
  - ✓ **Action Plan 12**：Enhance information security awareness and competence training

e-Government Program (2008-2011)

- **Flagship 2：National Information Security Technology Protection and Management Enhancement Program**
  - ✓ Establish government information security accreditation and certification system, developing government information security standards and enhance government institute information security management ability
  - ✓ Put data security protection into practice; enhance web application security quality
  - ✓ Strengthen information communication security report and response mechanism, enhancing information communication security report and response mechanism performance, assisting government agencies in handling major information security incidents and reducing impacts and loss from information security incidents
  - ✓ Establish information security incident early warning and response protection technology, enhancing information security early warning ability, providing information security trend evaluation and analysis to discover information security threat in time and reducing information security risks
  - ✓ Enhance public officials information security awareness and improve their information security competence
  - ✓ Participate in international information communication security joint defense mechanism, establishing transnational cooperation model and enhancing overall protection ability

Performance Indicators

Performance indicator	Indicator values				Explanation
	2008	2009	2010	2011	
Percentage which passed information security management certification standards	30%	50%	65%	75%	Proportion of A and B level institutions that passed government information security management certification tests
Information security intelligence shared on the governmental information security intelligence exchange platform	2	3	6	9	Establish information security intelligence networks with governmental backbone networks (such as GSN and TANET), professional management institutions, civil ISPS, and information security businesses
Time between updates of internet information security threat protection information	24 hours	12 hours	6 hours	3 hours	Time needed to upload blacklisted relay-stations on to government surveillance equipment
Independently researched and developed information security surveillance equipment in operation	80 units	90 units	100 units	120 units	The amount of information security equipment in operation which was independently researched and developed (Includes SOC, DNS warning system, user-end warning systems, intranet warning systems, Honeynet, and Botnet detection equipment)
Satisfaction score of information security services	80 points	85 points	88 points	90 points	Overall level of satisfaction of information security services provided to the government (Highest possible score is 100 points)

Challenges

- **Overall Strategy-Overall planning for national security strategy**
- **Budget Funds-The investment in information security affairs is still not enough**
- **Organization & Personnel-The professional ability of information security personnel needs improvement**
- **Technical R&D-The quality of autonomous technology and software needs further improvement**
- **Technology Security- Technology security issues of the worldwide information industry**
- **Law& Regulation- The legal responsibility of Enterprise concerning information security is still not clear**
- **International Cooperation- Fight Internet crime, and unite regional defense, etc.**
- **Universal Awareness- Cultivation of universal information security awareness**

6. Issues

- **How can government enhance overall government information and communication security ability by integrating resources and capabilities of industry, government, academic and research? What are the enhancing programs and priorities in engineering, enforcement and education?**
- **How can government establish information security early warning mechanism to enhance overall national information security incident response and protection ability by integrating information security messages, technology and experience exchange among industry, government, academic and research?**

Q&A