Metrics and the USAID Model Information Systems Security Program (MISSP)

If something can't be measured, it can't be managed!

Presented by
James P. Craft
USAID IA Program Manager
jcraft@usaid.gov
202/712-4559

Agenda

- USAID's Information Systems Security Challenge
- USAID Response to Challenge
- Model Information System Security Program (MISSP)
- Micro- and Macro- Metrics at USAID
- Results
- What is a "Good" Metric
- Conclusion

ISS Challenge at USAID

- ISS identified as two material weaknesses
  - IG Audits highlighted ISS as a major agency problem
  - No existing ISS program
  - Major Financial System needed major improvement
  - Critical Systems were not certified/accredited
- More funded needed to address critical ISS issues
- No information systems security culture
- No measures -- no accountability

USAID Response

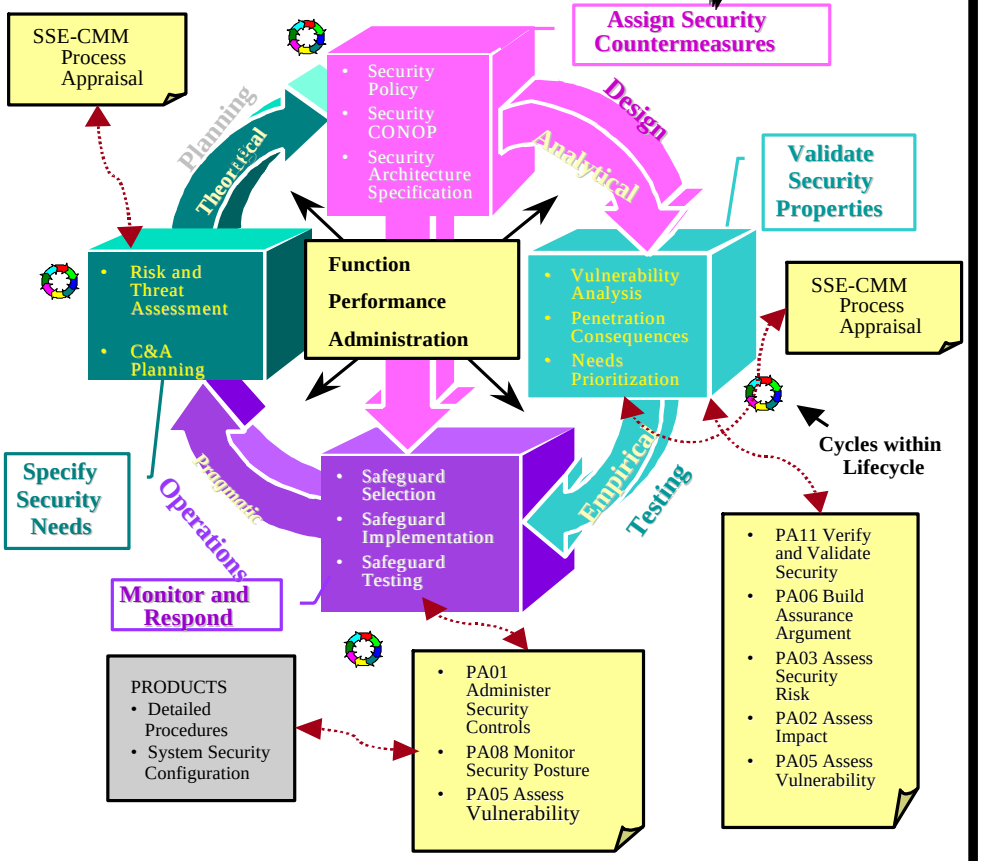
- Recruit Agency ISSO
- Set ISS vision and goals and develop USAID ISSP plan:
  - Security Process Framework - Program Areas with Life Cycle
  - Infuse Best Security Practices
  - Leverage external on-going ISS resources and activities e.g. MISSP
- Create MISSP to identify, collect, and implement Best Practices in standard format

MISSP Vision

- Freely Provide a Tested, Complete Model ISS Program
  - Rational functional & process frameworks
  - At least one best practice per essential ISS activity with practices tested in a global enterprise. Designed to be dynamically scalable to available resource level using alternative best practices
  - Modular design to include, policy, process, training, metrics, software, hardware, and tools- the MISSP Best Security Practice (BSP) Package
  - Use economies of scale & leverage national initiatives
- Bring Total Quality Leadership to ISS
  - Rapid prototype approach using multiple paradigms
  - Continual process improvement
- Metrics vision - highlight good and bad behavior

MISSP Implementation

SSE-CMM BASED ISS LIFE CYCLE → MAPS TO → MISSP BASELINE → MAPS TO → USAID REFERENCE IMPLEMENTATION



MISSP PROGRAM AREAS

- Security Program Management
- Personnel Security
- Security Training
- Physical Security
- Contingency Planning
- Technical Security
- Incidence Response
- Risk Management
- Certification and Accreditation
- Customer Security Support

USAID ISSPP

PRIME WBS

- PROGRAM AREA MANAGER ISS POLICY & PLANNING
- PROGRAM AREA MANAGER SECURITY TRAINING & AWARENESS
- PROGRAM AREA MANAGER ASSESSMENT
- PROGRAM AREA MANAGER OPERATIONS

USAID's MISSP "Rosette Stone"

USAID and MISSP

- MISSP Best Security Practice (BSP) approach is accelerating efforts to eliminate USAID security material weaknesses
- MISSP feeds and draws from USAID security efforts
  - To USAID: Security process framework (SPF), BSP package format, candidate BSPs e.g. security tools
  - From USAID: OIG reviewed BSPs for risk/vulnerability assessment, security training, intrusion detection, ISSPP, C&A
- MISSP approach has been adapted by the Federal CIO Council as its initiative (bsp.cio.gov)

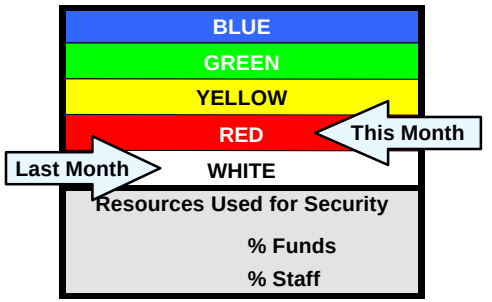
Micro-Metrics

- Technical and management measures
- Tactical Plans measures to BSP level metrics
- Implementation goals
- Tool results work great - Hydra, Cybercop
- Cost Benefit Analysis - failure of tool
- Failure of the ISS dashboard icon - will revisit
- TQL use focuses on schedule and cost for repeated application
- Leadership dynamic - democratization of metrics

USAID ISS Dashboard Icon

ISS ACTIVITIES THAT MUST BE COMPLETED	TO GO FROM
Security leads appointed & risk assessment conducted AND specific metrics developed for the task or system. Approved by ISS Team and/or ISSO.	White to Red
Task's security hours/costs programmed & security plan completed AND responsibilities and resources for completing metrics assigned.	Red to Yellow
ISS mechanisms/certification testing implemented & accredited AND key metric activities completed and tested. Accreditation based on DOD model.	Yellow to Green
ISS activities documented & artifacts prepared as best practice to export OR all metric activities completed, tested, documented as best practice.	Green to Blue

ISS ICON COLOR	MEANING
White	ISS Status UNKNOWN, Assumed that NO ISS Measures Exist
Red	No Planned ISS Activities Underway, Responsibilities Assigned
Yellow	ISS Measures Being Implemented BUT Measures NOT at Acceptable Level
Green	ISS Measures Tested, in Place, and Approved as Giving Acceptable Level of Risk
Blue	ISS Measures have been prepared for dissemination as ISS Best Practices



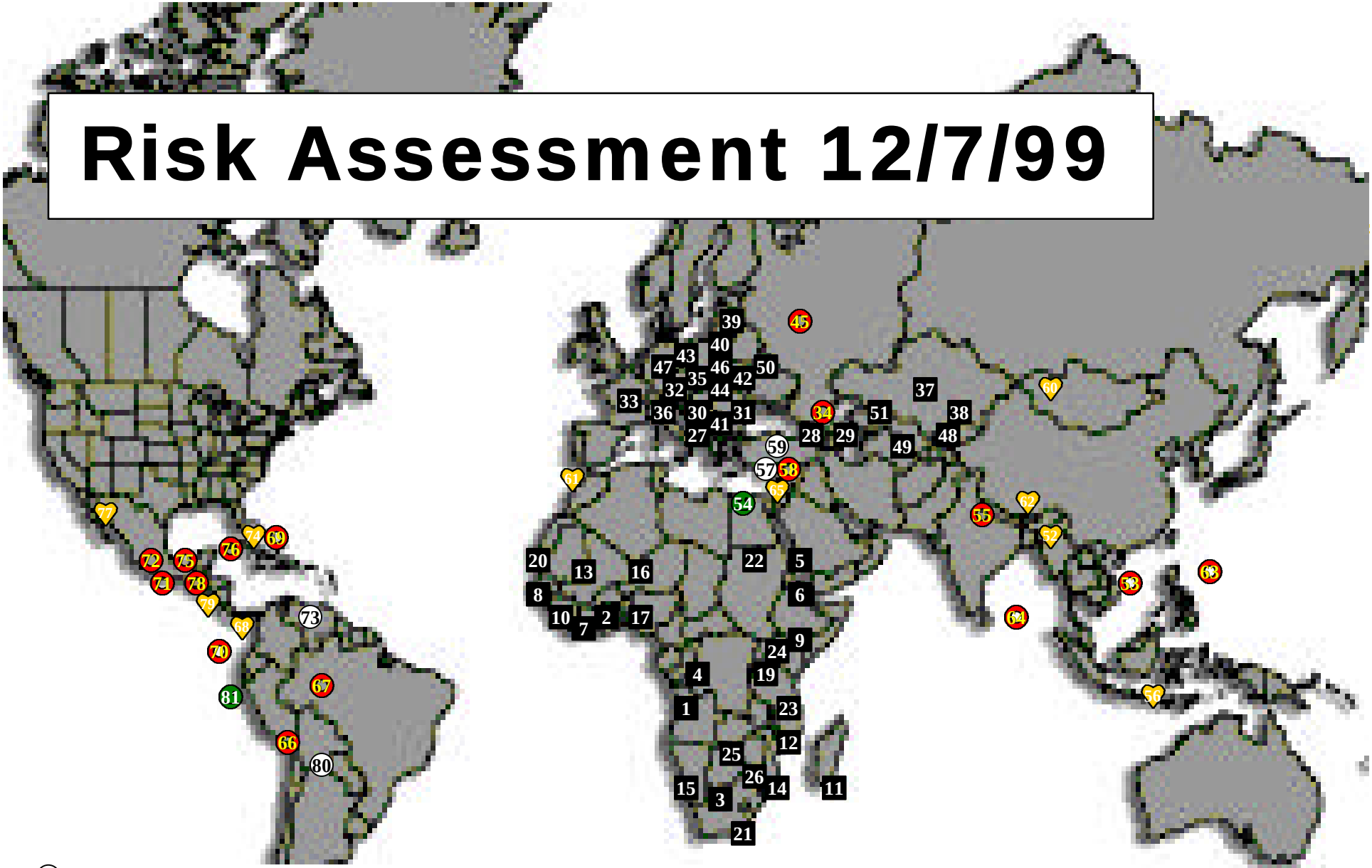
Language for inclusion into all contracts states:

- A risk assessment will be conducted (type and level of detail approved by ISSO)
- An individual will be designated to represent security concerns of the contact or task
- A security plan will be developed for the contract, its systems and applications
- Security mechanisms will be implemented and tested (certification)
- Formal approval will be obtained to operate Systems and Applications (accreditation)
- Security status will be reported monthly using the ISS Dashboard Icon

Macro-Metrics

- Program-wide and Agency-wide success
- Rollup of micro-metrics - bottom up approach
- Need to be simple to understand
- Material weakness and audit finding measures
- “Roadmap” progress coordinated with OIG
- Threat of shrinking budget, metrics as budget battle ammunition

Risk Assessment 12/7/99



White Identifies that no Computing resources exist.

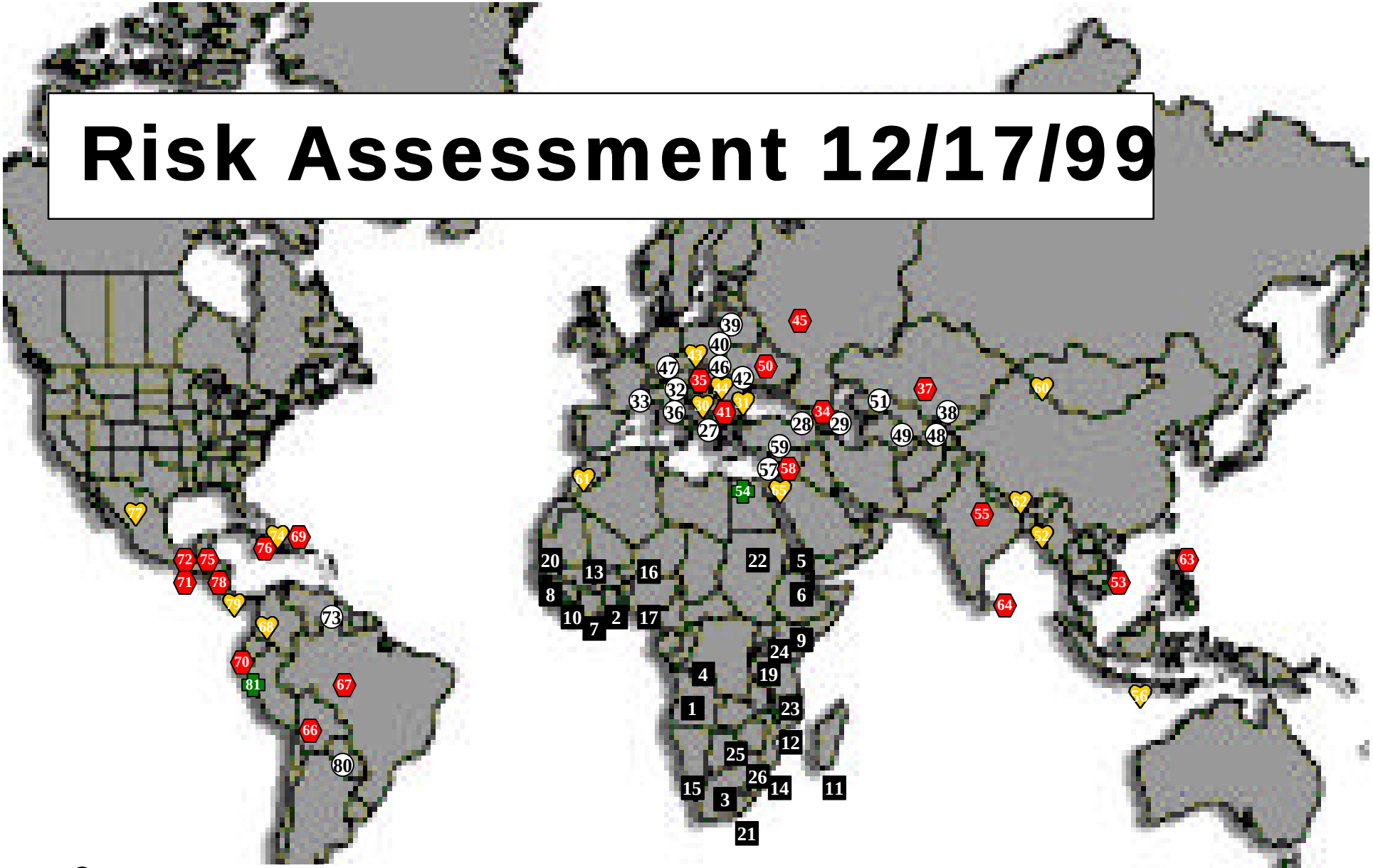
Identifies On-site Risk Assessment Activitv conducted.

Identifies that an Automated Scan was conducted and only Minor Vulnerabilities exist.

Identifies that an Automated Scan was conducted and High to Medium Vulnerabilities exist.

Identifies that no Risk Assessment Activity was conducted.

Risk Assessment 12/17/99



White Identifies no AIDNET connected Computing resources.

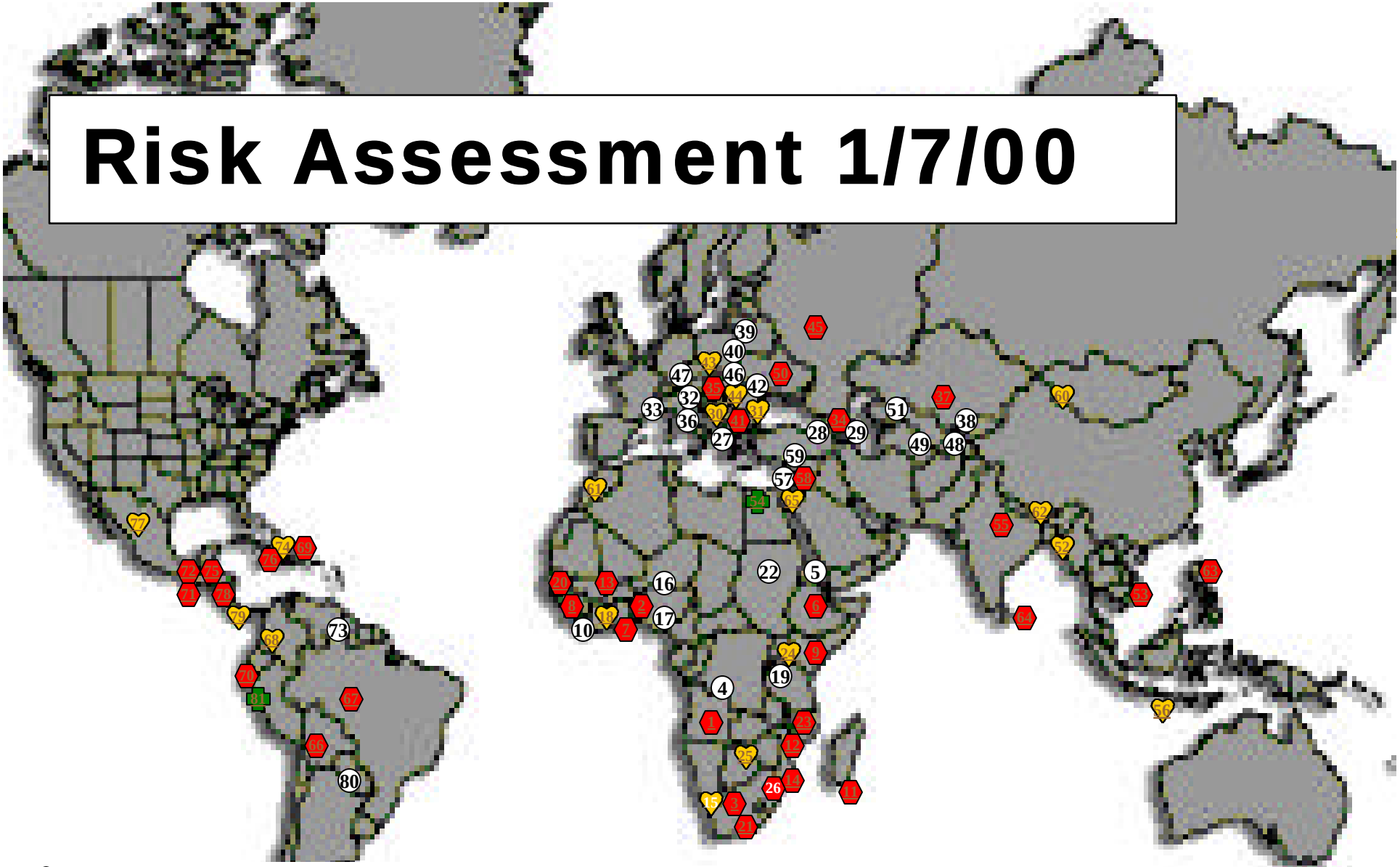
Identifies On-site Risk Assessment Activity conducted.

Identifies that an Automated Scan was conducted and only Minor Vulnerabilities exist.

Identifies that an Automated Scan was conducted and High to Medium Vulnerabilities exist.

Identifies that no Risk Assessment Activity was conducted.

Risk Assessment 1/7/00



White Identifies no AIDNET connected Computing resources.

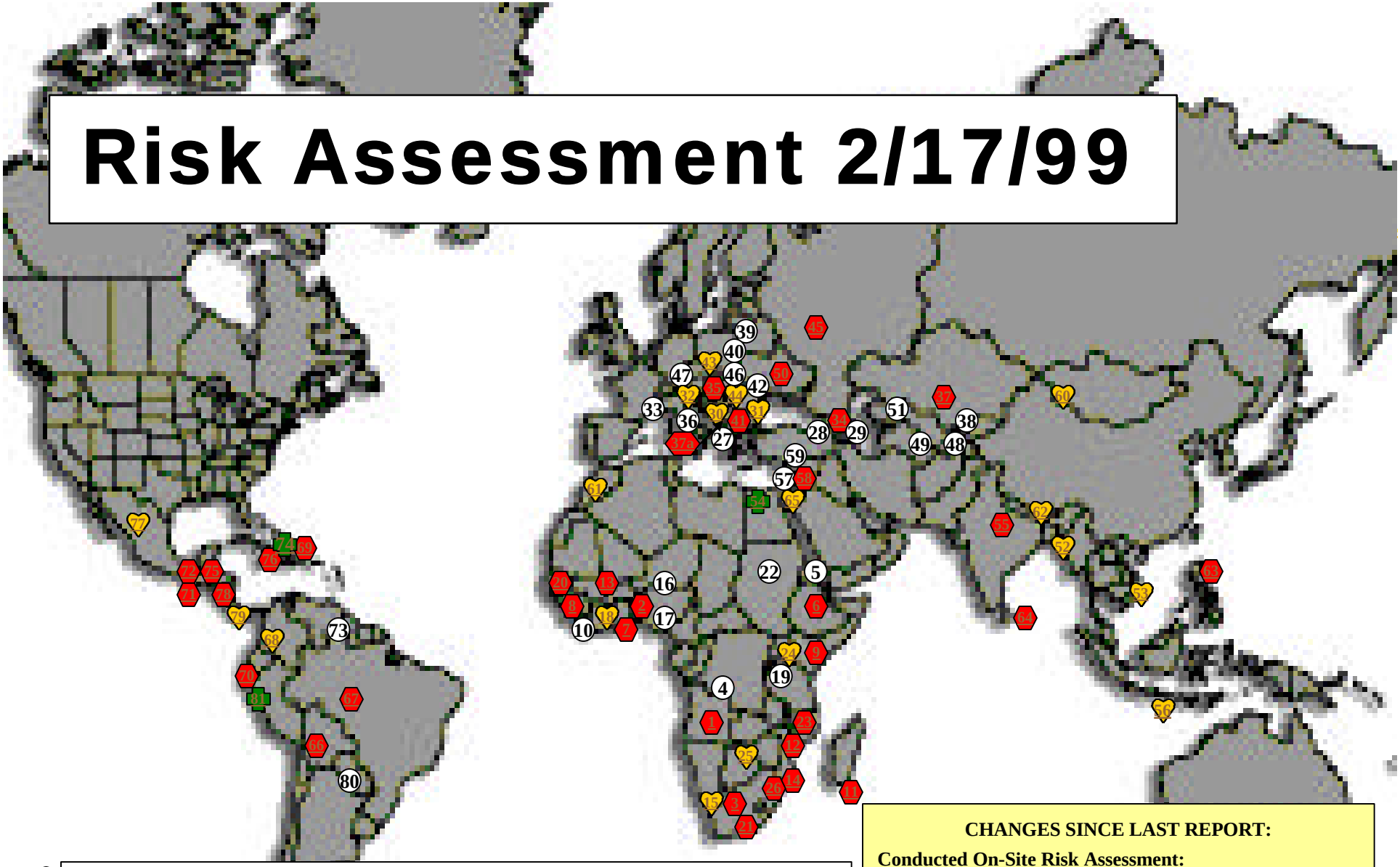
Identifies On-site Risk Assessment Activity conducted.

Identifies that an Automated Scan was conducted and only Minor Vulnerabilities exist.

Identifies that an Automated Scan was conducted and High to Medium Vulnerabilities exist.

Identifies that no Risk Assessment Activity was conducted.

Risk Assessment 2/17/99



White Identifies no AIDNET connected Computing resources.
Identifies On-site Risk Assessment Activity conducted.
Identifies that an Automated Scan was conducted and only Minor Vulnerabilities exist.
Identifies that an Automated Scan was conducted and High to Medium Vulnerabilities exist.
Identifies that no Risk Assessment Activity was conducted.

CHANGES SINCE LAST REPORT:

Conducted On-Site Risk Assessment:

GREEN => 74

Follow-up Scan Results:

Red => Blue: 31, 45

Red => Red: 34, 35, 55, 63, 67

Initial Scan Results:

Red => 37a

Africa

1.Angola
2.Benin
3.Botswana
4.Democratic Republic of Congo
5.Eritrea
6.Ethiopia
7.Ghana
8.Guinea
9.Kenya
10.Liberia
11.Madagascar
12.Malawi
13.Mali
14.Mozambique
15.Namibia
16.Niger
17.Nigeria
18.Cote D'Ivoire
19.Rwanda
20.Senegal
21.South Africa
22.Sudan
23.Tanzania
24.Uganda
25.Zambia
26.Zimbabwe

Europe and Eurasia

27.Albania
28.Armenia
29.Azerbaijan
30.Bosnia and Herzegovina
31.Bulgaria
32.Croatia
33.France
34.Georgia
35.Hungary
36.Italy
37.Kazakhstan
37a Kosovo
38.Kyrgystan
39.Latvia
40.Lithuania
41.FYR of Macedonia
42.Moldova
43.Poland
44.Romania
45.Russia
46.Slovakia
47.Switzerland
48.Tajikistan
49.Turkmenistan
50.Ukraine
51.Uzbekistan

Asia and the Near East

52.Bangladesh
53.Cambodia
54.Egypt
55.India
56.Indonesia
57.Israel
58.Jordan
59.Lebanon
60.Mongolia
61.Morocco
62.Nepal
63.Philippines
64.Sri Lanka
65.West Bank and Gaza

Latin America and the Caribbean

66.Bolivia
67.Brazil
68.Colombia
69.Dominican Republic
70.Ecuador
71.El Salvador
72.Guatemala
73.Guyana
74.Haiti
75.Honduras
76.Jamaica
77.Mexico
78.Nicaragua
79.Panama
80.Paraguay
81.Peru

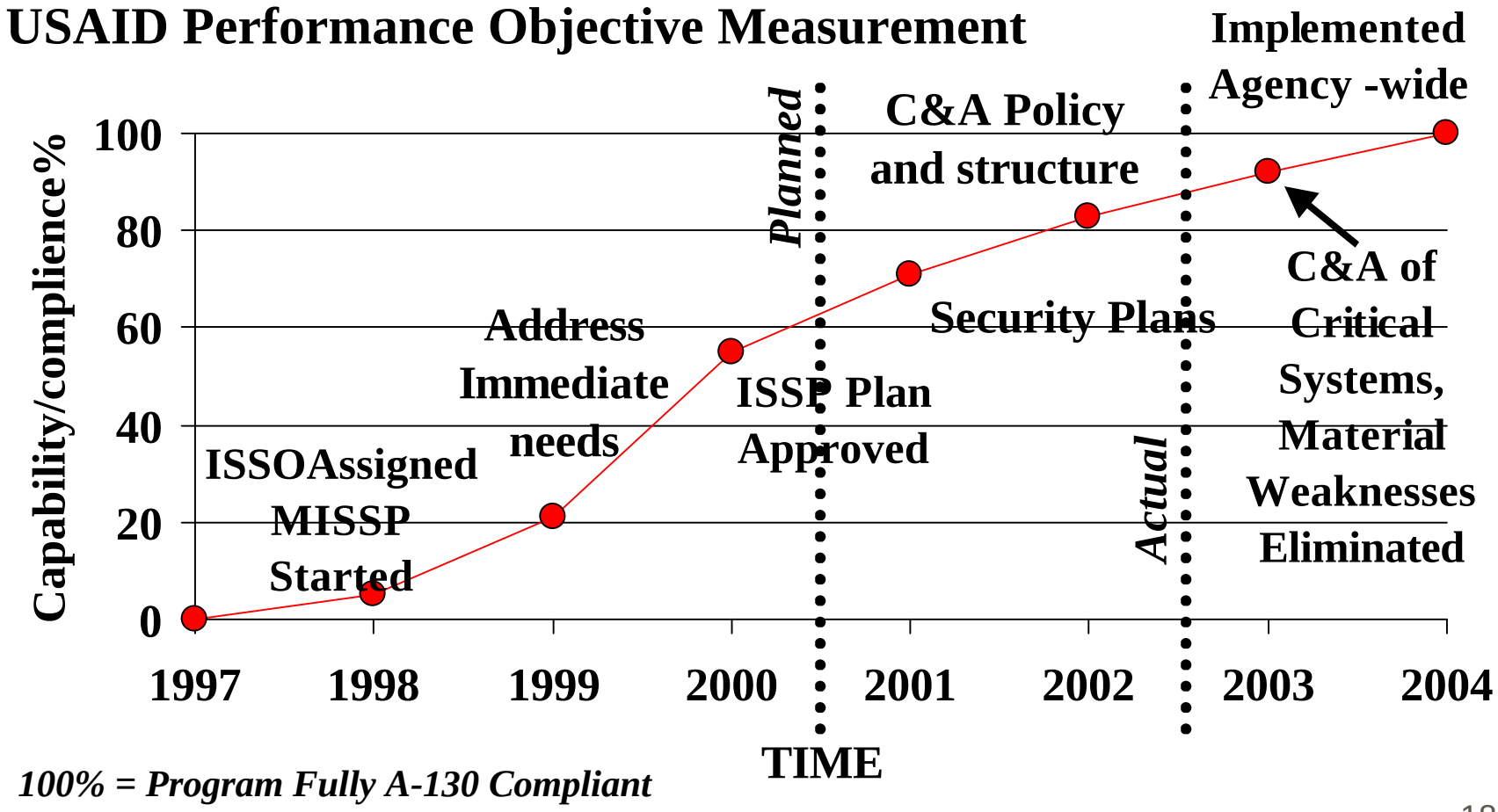
Specific Results

- Engineered stronger systems security controls
  - For major system (NMS) and GroupWare (Lotus Notes)
- Developed USAID's security risk assessment/site support BSPs - exporting ISS to USAID missions worldwide and now developing countries central banks
- Integrated security into USAID Target Information Technology Architecture
- Increased support throughout Agency

Specific Results

- Maintaining security under escalating attacks
- Strengthened USAID's WAN perimeter safeguards (Firewall, RAS)
- Speeding the fielding of standard ISS products Agency-wide (anti-virus, RAS, PKE, IDS, etc.) and cutting costs
- Total Quality Leadership principles creating a process-driven security culture
- Now moving to support international development work

Planned & Actual Results



100% = Program Fully A-130 Compliant

What is a “Good” Metric

- Easy to collect
- Maps to business goals and strategy
- Useful input to a decision
- Identifies who it is aimed at
- Fits into an accepted model for using organization
- Highlights good and bad behavior
- Flexible but objective

Conclusion

- USAID is benefiting from a TQL Metrics-based approach and believes that others can also
  - Leverages federal and national level initiatives
  - Program investments showing measurable returns
  - Helping USAID respond to staff and budget cuts
  - Focuses on a leadership paradigm
- Pragmatic metrics use (bottom up) tailored to culture seems to offer best results
- Using the Federal CIO Council Best Security Practice to help support metrics use in government and industry