Appendix C:
Summary of Recommendations

1. The Commission recommends enactment of a statute establishing the principles on which Federal classification and declassification programs are to be based. (p. 13)

2. The Commission recommends that the Security Policy Board (SPB) implement within one year the Joint Security Commission recommendation on establishing a single set of security standards for special access programs (SAPs). The SPB, in conjunction with the Department of Defense, should examine whether the National Industrial Security Program Operating Manual Supplement should continue to allow individual SAP program managers to select the security measures for their program rather than conform to a single standard. Industrial contractors should be included in this review and in the development of a single set of standards. (p. 28)

3. The Commission recommends that agencies take several steps to enhance the proficiency of classifiers and improve their accountability by requiring additional information on the rationale for classification, by improving classification guidance, and by strengthening training and evaluation programs.

Elements of this approach should include:

- •Original classifiers shall provide a detailed justification for each original classification decision;
- •Derivative classifiers shall be required to identify themselves on the documents they classify;
- •Classification guides shall be better developed, more definitive, and updated regularly, and industry shall participate in the preparation of guides affecting industrial programs;
- •Training shall be expanded to include derivative classifiers and shall conform to minimum Executive Branch standards; and
- •Proper classification of information shall be included as a critical element in the performance evaluations of *all* employees authorized to classify. (p. 34)

4. The Commission recommends that classification decisions, including the establishment of special access programs, no longer be based solely on damage to the national security. Additional factors, such as the cost of protection, vulnerability, threat, risk, value of the information, and public benefit from release, could also be considered when making classification decisions. (p. 38)

5. The Commission recommends that responsibility for classification and declassification policy development and oversight be assigned to a single Executive Branch body, designated by the President and independent of the agencies that classify. This entity should have sufficient resources and be empowered to carry out oversight of agency practices and to develop policy. Based on its oversight findings, this body would then make recommendations for policy and implementation of classification and declassification issues directly to the National Security Council. The Security Policy Board would have an opportunity to comment on these policy recommendations through the NSC process. (p. 44)

6. The Commission recommends the creation by statute of a central office—a National Declassification Center—at an existing Federal agency such as the National Archives and Records Administration to coordinate national declassification policy and activities. This Center would have the responsibility, authority, and funds sufficient to coordinate, oversee, and implement government declassification activities. The Center would monitor agency declassification programs and provide annual reports on their status to the Congress and the President. (p. 68)

7. The Commission recommends that the use of sources and methods as a basis for the continuing classification of intelligence information be clarified through issuance of an Intelligence Community directive by the Director of Central Intelligence, explaining the appropriate scope of that protection. (p. 70)

8. The Commission recommends that agencies better structure their records management and systematic declassification programs to maximize access to records that are likely to be the subject of significant public interest.

Elements of this proposal should include:

- •Complying with the dates or events for declassification, including through the use of new technologies;
- •Consolidating and regularly updating declassification guidance that is easily accessible to those authorized to declassify within the agency;
- •Prioritizing declassification according to entire record groups selected through active consultation with the public and outside scholars, and regularly informing the public of systematic review results;
- •Requiring all offices with any declassification-related activities to demonstrate that they are operating in partnership with others in the agency involved in related activities; and
- •Establishing ombudsman offices in each agency that has original classification authority or engages in declassifying records: these offices would intervene in and resolve classification and declassification issues upon request, act as a conduit for public concerns about access to records, and, where appropriate, refer issues to the agency's Inspector General. (p. 71)

9. The Commission recommends five guiding principles as the essential elements of an effective personnel security system. Most already are part of the current system (including under Executive Order 12968), but too often they are not actually practiced throughout the Federal Government. The Commission recommends that these standards be incorporated into a new statute or regulation that would supersede Executive Order 10450.

The five guiding principles are:

- •Openness and clarity of standards;
- •Balanced, "whole-person" standards;
- •Reciprocity for classified access;
- •Nondiscrimination principles; and
- •Assurances of due process. (p. 80)

10. The Commission recommends that individuals in both Government and industry holding valid clearances be able to move from one agency or special program to another without further

investigation or adjudication. The single exception to this true reciprocity of security clearances shall be that agencies may continue to require the polygraph before granting access. (p. 82)

11. The Commission recommends that current requirements for neighborhood interviews and for interviewing educational references in every investigation be eliminated. (p. 86)

12. The Commission recommends that greater balance be achieved between the initial clearance process and programs for continuing evaluation of cleared employees. (p. 87)

13. The Commission recommends that both the Congress and the Executive Branch reevaluate the requirement to utilize a new financial disclosure form and consider staying its implementation until there is further evaluation concerning how it would be used and whether its benefits exceed its costs. The Congress and the Executive Branch should review alternative approaches to improving data collection, including utilization of the expanded access to certain financial and travel records provided for under Executive Order 12968. (p. 89)

14. The Commission recommends that: (1) the director of scientific research at the Department of Defense Polygraph Institute establish a committee that includes cleared, outside scientific experts to develop a coherent research agenda on the polygraph; initiate and participate in a small grant program to stimulate independent research outside the Government; and review and comment on scientific progress and the quality of government-sponsored research in this field; and (2) independent, objective, and peer-reviewed scientific research be encouraged as the best means to assess the credibility of the polygraph as a personnel security tool and identify potential technological advances that could make the polygraph more effective in the future. (p. 91)

15. The Commission recommends revising the Computer Security Act of 1987 to reflect the realities of information systems security in the Information Age.

Some of the changes to the Act might include:

- •Moving the Computer Systems Laboratory from the National Institute of Standards and Technology to a higher visibility position within the Commerce Department, thereby increasing the likelihood of funding and personnel to support the civilian side of Government;
- •Directing agencies to set aside specific funds, perhaps as a budget line item, for information systems security training; and
- •Requiring the Office of Personnel Management to create a career path for information systems security professionals that includes network administration and computer crime investigation. (p. 104)

16. The Commission recommends developing an information systems security career path across the Government. (p. 111)