Polygraph

VOLUME 35 2006 NUMBER 4

Contents

Published Quarterly

P.O. Box 8037, Chattanooga, Tennessee 37414-0037

Behavioral, Psychological and Physiological Aspects of Security Evaluations: Report on a Series of Workshops[1]

National Science Foundation (NSF) and
Office of Science and Technology Policy (OSTP)

Abstract

The accuracy of security evaluations is of vital concern to Federal agencies. Accurate security evaluations serve to protect the Nation's well-being while also protecting the rights of individuals. Historically, security evaluations utilized polygraphs ('lie detectors') and other tools, but the scientific validity of the polygraph has been questioned. In 2003 the National Research Council (NRC) of the National Academies published a volume critical of reliance on a technique with an imperfect ability to detect deception. That report also indicated that inaccurate results have the potential to both compromise national security and to do grievous harm to the lives of innocent individuals.

To explore these methods further, Congress mandated that NSF and OSTP conduct a series of workshops. An Interagency Advisory Group (IAG) was formed to identify topics for exploration and individuals with scientific and practical expertise in these areas, and six NSF-supported workshops were held to move toward developing a research agenda. Each workshop focused on a different science-based approach to the central question of scientifically valid techniques to conduct security evaluations. The workshops brought together researchers and practitioners to discuss theory and innovative scientific developments, as well as real-world applications of the technology. At each workshop, additional discussion revolved around several core questions, such as ethical and privacy concerns, cross-cultural adaptability, and contextual factors. This report summarizes the findings from these workshops and includes a catalogue of relevant federally-funded research that was developed as part of these efforts.

A number of major themes emerged across the six workshops that can help guide future research.

Theoretical and Empirical Foundations

Currently there is little development of theoretical models for explaining links between human reactions—whether they are hormonal, neural, linguistic, or behavioral—and deception. As research progresses, it must inform the development of theoretical underpinnings, which in turn will guide future research.

Establishment of Standards and Scenarios

There is a clear need for the creation of standardized protocols for assessing deception so that various techniques can be appropriately compared and evaluated.

High-Quality Data

A scientific approach to security evaluations requires high quality data. Research can be hampered by use of inappropriate research participants, small sample sizes, and proxies that are poor

[1] Reprinted with permission of the National Science Foundation.

representations of real-world situations. Researchers repeatedly emphasized that access to additional data on actual security compromises would be exceptionally useful in the design and testing of new approaches.

Roles of Culture, Gender, Language, Geography, Acculturation, and Individual Differences

It is imperative to investigate the role of variables such as culture, gender, language, geography and individual variation in security evaluation. Behavior viewed as deceptive in one cultural context might not be viewed as such in another context. The cultural perception of what constitutes lying can vary from place to place. The degree to which results can be generalized is a key concern.

New Training Paradigms

There is a need to foster the development of a means to train researchers in the relevant areas. Training opportunities should be available across a wide range of levels, from undergraduates through established scholars. Increasing opportunities to embed researchers in applied settings and practitioners in research settings will help significantly to move both research and practice forward.

Social/ Ethical/ Legal Issues

Legal, political and ethical considerations must be included in the dialogue concerning deception detection. In particular, individual privacy and confidentiality are inherently at risk.

Deterrence

Polygraphy has preventative value as a deterrent. There is a need for a better scientific understanding of the deterrent effect and how to best utilize this effect.

Sensor Development/ Encoding Technology

A plethora of potential indicators of stress may be linked with deception. It is critical that scientists engage in collaborative research to develop the most effective means of capturing and assessing behavioral characteristics that may be linked with deception.

Infrastructure

Coupled with the need for high quality data and assessment tools, development of cyberinfrastructure with the capacity to aggregate multiple channels of information and to conduct large-scale data mining is critical.

In addition to the generally applicable themes, each workshop identified promising short and long-term research avenues. These range from the development of dictionaries of symbolic gestures and facial expressions for cultures of interest, to aggregating and mining extensive disjointed sources of data for risk management, to the use of neuroimaging technologies for fundamental understanding of deception.

The series of Interagency Advisory Group meetings and NSF/OSTP workshops was designed to consider the findings of unclassified research to date, catalogue and coordinate Federally funded research activities, and develop short-term and long-term research agendas for coordinating Federally funded research.

Charge to NSF and OSTP

The Intelligence Authorization Act for Fiscal Year 2004, 1.5.1.3 Section 375: "Coordination of Federal Government Research on Security Evaluations," stated that:

> "The National Science Foundation and the Office of Science and Technology Policy shall jointly sponsor not less than two workshops on the coordination of Federal Government research on the use of behavioral, psychological, and physiological assessments of individuals in the conduct of security evaluations."

The purposes of the workshops were:

> "(1) To provide a forum for cataloging and coordinating Federally funded research activities relating to the development of new techniques in the behavioral, psychological, or physiological assessment of individuals to be used in security evaluations.
>
> (2) To develop a research agenda for the Federal Government on behavioral, psychological, and physiological assessments of individuals, including an identification of the research most likely to advance the understanding of the use of such assessments of individuals in security evaluations.
>
> (3) To distinguish between short-term and long-term areas of research on behavioral, psychological, and physiological assessments of individuals in order to maximize the utility of short-term and long-term research on such assessments.
>
> (4) To identify the Federal agencies best suited to support research on behavioral, psychological, and physiological assessments of individuals.
>
> (5) To develop recommendations for coordinating future Federally funded research for the development, improvement, or enhancement of security evaluations."

Federal Agency Involvement in the Planning Process

The Interagency Advisory Group (IAG) was formally assembled in response to requests from OSTP and NSF to include each of the agencies mentioned in the statutory language. However, over the course of the workshops and additional meetings, Federal involvement grew much broader. Individuals from each of these agencies had some contact in planning and/or attending the workshops.

Department of Justice (DOJ)

- Attorney General (AG)
- Federal Bureau of Investigation (FBI)
- National Institute of Justice (NIJ)

Central Intelligence Agency (CIA)

Department of Defense (DOD)

- Defense Advanced Research Projects Agency (DARPA)
- Defense Intelligence Agency (DIA)
- Counter Intelligence Field Activity (CIFA)
- Defense Personnel Security Research Center (PERSEREC)
- Department of Defense Polygraph Institute (DODPI)
- Office of Naval Research (ONR)

Department of Energy (DOE)

Department of Homeland Security (DHS)

Department of State (State)

Executive Office of the President (EOP)

Office of National Counterintelligence Executive (NCIX)

Office of Science and Technology Policy (OSTP)

National Institutes of Health (NIH)

National Science Foundation (NSF)

National Security Agency (NSA)

Office of Personnel Management (OPM)

NSF/OSTP Sponsored Workshops

As mandated by the Act, NSF and OSTP formed an Interagency Advisory Group (IAG) with representatives from the agencies identified by the Act: the National Science Foundation, Office of Science and Technology Policy, Department of Defense, Department of the Secretary of State, Attorney General's Office, Department of Energy, Department of Homeland Security, Central Intelligence Agency, Federal Bureau of Investigation, and National Counterintelligence Executive.

The Interagency Advisory Group (IAG) decided which topics and issues were relevant to behavioral, psychological, and physiological assessments of individuals in security evaluations. Although the security evaluations backlog for worker clearances is a critical operational challenge, the kinds of problems, relevant behavioral, psychological, and physiological variables, and scientific issues identified in the context of clearance evaluations extended across a wide range of situations.

The IAG identified six scientific domains relevant to security evaluations and decided to have one workshop for each. The six foci corresponded to the domain areas mandated by the Act ("behavioral, psychological, and physiological") with some further divisions within these domains. The IAG suggested scientists and operational field individuals for each workshop and NSF made grants to scientists to lead each.

The six workshops were:

(1) Language and Deception in Security Evaluations, June 2-3, 2005

(2) Behavioral Measures in Security Evaluations, June 27-28, 2005

(3) Emerging Technologies in Security Evaluations, July 13-14, 2005

(4) Autonomic and Somatic Measures in Security Evaluations, July 18-19, 2005

(5) Psychological Assessments in Security Evaluations, July 25-26, 2005

(6) Functional Brain Imaging in Security Evaluations, August 1-2, 2005

In addition to its own particular focus, each workshop was specifically asked to address the following set of important issues that cut across all six topic areas:

(i) cross-cultural and multicultural issues, including the use of translators

(ii) issues of gender, race and ethnicity

(iii) privacy concerns

(iv) ethical concerns – information sharing, false positives, false negatives

(v) how models and methods from other fields might be applicable to the problems encountered in this domain

(vi) situational/contextual factors

(vii) international research and practice

(viii) innovative new approaches

Following the six workshops, the leaders (Principal Investigators, PIs) of each workshop convened August 15, 2005 to create a preliminary summary of the workshops. A plenary workshop held on October 3, 2005 brought key members of each of the topic-focused workshops together to share information and discuss overall recommendations, and a final meeting by the IAG considered these recommendations on October 20, 2005. A draft report to NSF and OSTP was prepared by MITRE Corporation as part of the NSF grant for the final plenary workshop. The draft served as a resource in preparing this report. Appendix A describes the development of and funding mechanisms for the workshops in greater detail.

The goal of each workshop was to review the science in each topical area, explore the most innovative research in those areas, develop a short- and long-term research agenda for the Federal Government and identify the research most likely to advance the understanding of assessments of individuals in security evaluations. Participants in each workshop were also asked to identify Federal agencies to support such research and recommend how to coordinate such research. The outcomes from the workshops are summarized below.

The Challenges

Security Evaluation Contexts

The security evaluations backlog for employee clearances is a critical operational challenge, and the many contexts in which security must be assessed compounds the difficulties. The workshop participants focused on the evaluation efforts in a number of these situations, including:

Federal and private security clearance

Airport security, border-crossing security

Local law enforcement

Difficult intelligence problems

Pre-employment screening

Intelligence asset evaluation

Basic Sources of Information to be Considered

In each of these situations, human data are examined with the intent to make inferences about deception, integrity, lying, identity, and national security risk so that the security evaluation will prevent and deter security breaches. Psychological, physiological and behavioral data were the focus of these workshops, as well as the behavioral traces of past behavior and data accumulated in the present. Specifically, the sources of data that emerged across the workshops include:

Past Behavior (Behavioral Trace)

Public records – property ownership, driver's license, other licenses

Private records – credit reports, travel records, phone records

Written records – e-mails, Instant Messaging (IM), letters

Recorded conversations, transcriptions, overheard conversations, phone calls

Third party interviews – biographic information, peer report, supervisor's report

Security cameras/street cameras

Present Behavior – Verbal and Non-verbal Behavior

Observations at border crossing or airport

Interview at border crossing or airport security checkpoint

Interview for employment

Interview for security evaluation, clearance

Law enforcement

Present Behavior – Augmented Interview Data

Contact recordings – electrodermal response, heart rate, respiration, blood pressure, etc.

Non-contact recordings – thermal imaging, voice quality, body odor, components of breath, eye movements, analysis of facial muscle movement

Brain recordings – fMRI, evoked potential, etc.

Combined Information

Federal security evaluation decisions are ultimately human decisions, usually achieved through a process of adjudication that weighs combined information from past behavior, verbal and non-verbal behavior, and perhaps polygraph and other augmented interview measures. Thus, the quality of each specific measure is important, but so is creating a quality process for combining different sources of information to make a security decision. Repeatedly across the workshops aggregations of multiple sources of information were reported to be more accurate than relying on information from a single source. The 2003 report by the National Research Council, *The Polygraph and Lie Detection*, presented the relevant issues related to combining information from different sources. Information can be collected simultaneously (independent parallel testing), or sequentially (independent serial testing), and can be aggregated by human judgment, computer algorithm, or other decision support tools. This was flagged as an area in need of additional research.

Workshop questions that emerged around this issue of combining information were as follows:

- What are optimal strategies for combining information using humans and computers?
- How best can humans be trained to combine information effectively?
- Who inherently possesses good skills at combining information and what thought processes make them expert?
- How can multi-stage assessments be used effectively,– beginning with less invasive assessments?
- How can adjudication be informed by decision science?

Multidimensional Space

Workshop participants determined that identification of the security risks posed by an individual depends on where that individual resides in a multidimensional space that may change with time. Relevant dimensions of this space include:

- The security context and the degree of associated risk (e.g., pre-employment screening, visa applications, border crossings)
- Characteristics of the individual, including motivations (e.g., people may be volunteering information for employment; testing security systems as an intellectual challenge or gaming; hiding information without intent to harm or deceive; or hiding information or providing misleading or erroneous information with intent to harm)
- The ease with which critical information can be obtained (e.g., open source, shared source, classified)
- Cultural, political and economic milieu
- Varying timescales for assessment (e.g., brief assessment of passengers at airports to lengthy employment interviews)

Basic Sciences Involved in Security Evaluations

Per instruction from Congress, the focus was on the psychological, physiological, and behavioral aspects of security evaluations. This is necessarily broadly multidisciplinary work. In fact, it was suggested that a new multidisciplinary field of security science might emerge to pool the necessary expertise across multiple disciplines. This may be reflected in emerging professional

associations, journals, and regular meetings. Relevant areas important in psychological, physiological and behavioral aspects of security evaluation include:

Clinical psychology

Cognitive neuroscience

Communications

Computer and information science

Criminal justice / criminal science

Decision science

Developmental psychology

Geography

Human cognition and perception psychology

Industrial organization psychology

Laws, Ethics, and Society

Linguistics and computational linguistics

Physical and cultural anthropology

Psychophysiological psychology

Risk and risk management

Social psychology

Sociology

A primary concern of all the workshops was that, as the technology supporting these sciences becomes increasingly effective, legal and ethical issues are likely to become greater challenges. It was concluded that policies and practices for addressing these issues are as important to develop as the underlying sciences and relevant technologies. It is also important to note that the research on psychological, physiological, and behavioral aspects of security evaluation also has links to other social and behavioral sciences, including political science, geography, and economics, as well as links to other sciences such as biology and mathematics.

Discoveries with multiple uses beyond understanding deception will be a beneficial consequence of investigations into the science underlying security evaluations. For example, these sciences will help us understand many of the basic psychological and physiological processes of cognition, emotion and motivation, which will be relevant to physical, mental and social health and disease.

Major Emerging Issues

Major themes emerged out of the workshops and IAG meetings that were not linked to specific workshop topics. Summarized here are the major crosscutting emerging issues. Each of these offers significant research opportunities and an opportunity for investment in the scientific understanding of security evaluations from multiple perspectives, namely behavioral, psychological and physiological. Additional suggestions follow in the discussion of each specific workshop.

Theoretical and Empirical Foundations

There is a clear need for unified behavioral and physiological models; combinations of cognitive models, neural models, and psychophysiological models will help lead the science in promising directions. Work that is currently *ad hoc* will be much more focused and insightful when guided by an empirically grounded theory. Fostering the development of theoretical models will be a major step in driving new discoveries as such models would help with the crucial tasks of understanding the links between deception and stress, arousal, fear, anger, and attention.

Establishment of Standards and Scenarios

Standard protocol ”test-bed” scenarios must be developed for assessing deception and its detection. These will allow fair comparisons across conditions and across laboratories and will contribute to data quality. A standardized approach will allow for assessment of new products and protocols. A working group should develop laboratory scenarios, including rigorous, high-stakes

problems. Product evaluations that meet the standards reflected in peer-reviewed research will serve as significant research infrastructure and allow for effective investment of public funds.

High Quality Data

High quality and sufficient data are a necessity. Current research is hampered by the use of scientifically inappropriate samples of research participants and insufficient sample sizes (often small numbers of college students). Further, the laboratory-based experiments that attempt to simulate deceptive behavior are poor stand-ins for real world data and do not represent truly stressful and compromising situations. Data on actual security compromises are seldom available for academic researchers, yet, in a sanitized form, could be very useful for building the peer reviewed body of knowledge.

Data repositories are necessary -- they accumulate large sets of data that can be useful both for testing research hypotheses and as a basis for comparison with new data. Research in security evaluations will move forward with data repositories that make available indexed data backed by assurances of data quality. For example, a very large accumulated language corpus obtained when people are attempting to deceive can serve as a background for analysis of new language samples.

The research, practitioner and ethical/legal communities must engage in further discussion of seemingly contradictory needs and requirements. For example, there are requirements to operate experiments in accordance with the Common Rule (the standard for regulating human research), but also a clear need for deception experiments that must use human subjects. On some campuses, research is hampered by Institutional Review Boards (IRB) that may not fully understand the risks and benefits of this work, and thus may limit security evaluation research in ways not called for by the Common Rule. For example, some IRBs are reluctant to waive informed consent, or documentation of informed consent, even though the Common Rule gives them the flexibility to do so.

In addressing the scientific investigation of deception, researchers repeatedly emphasized the importance of accessing real-world behavioral data with real consequences and known outcomes.. Researchers and practitioners will need to develop strong partnerships to overcome the present legal, political, social, practical and financial constraints of using real world data.

Roles of Culture, Gender, Language, Geography, Acculturation, and Individual Differences.

Deception, and the psychological, physiological, and behavioral indicators of compromised security, is not manifest in universal ways. For instance, research has suggested that there may be significant cultural differences in gaze aversion during lying. A behavior perceived as deceptive in one culture or geographic location may not be viewed as deceptive in another. Assessments and implementation protocols must take into account not only cultural variability and the degree of acculturation of an individual, but also gender and linguistic differences among individuals. What are the cultural values of lying, and how is deception adaptive in a particular context or culture? Are there differences between women and men in correlates of deception, and do these vary with cultural geography? Although it is often assumed that physiological responses are less variable across cultures than responses based on language or facial expression, this is unsubstantiated.

New Training Paradigms

These workshops brought together scholars and practitioners in unusual combinations, with exceptionally promising results. One result of these collaborative arrangements was the recommendation for greater opportunities for knowledge exchange through embedded positions. When practitioners can spend time in research labs, they gain an appreciation for the scientific process and are in a position to introduce a practical bent to the research, while providing considerable accumulated and highly practical wisdom. When researchers spend time in practical security evaluation settings they gain an appreciation for the ultimate application

contexts of their research, are in a position to introduce a rigor to field assessments, and bring a command of the research literature to the field settings. Such exchange sets the stage for further forums for interaction.

There is a small community of researchers currently focused on physiological, psychological, and behavioral aspects of security evaluation and there was a clear expression of the need to bring along the next generation of scholars and practitioners. A focus at the undergraduate, graduate and postdoctoral levels was emphasized.

Social/Ethical/Legal Issues

The workshops reviewed the legal, political, and ethical considerations in deception detection and participants unanimously recommended continuing dialogue among researchers, ethicists, legal scholars and members of the public. Privacy and confidentiality are inherently at risk as public and private behaviors are scrutinized, and rights are given up for the privilege of crossing borders or flying on airplanes.

Assessments of individuals who are seeking security clearance in the conduct of their work for the United States Government raise fewer legal and ethical questions than assessments in other circumstances, as those seeking security clearance necessarily give permission for confirmation of information. These security clearance assessments do, however, raise issues about the privacy and confidentiality of third party individuals.

Deterrence

Part of the success of polygraphy is its preventive value as a deterrent. There is a need for a better scientific understanding of the deterrent effect and how best to take advantage of this effect.

Sensor Development/Encoding Technology

There are hundreds of potential indicators of stress that may be linked with deception. Researchers and engineers may need to develop hundreds of items of associated hardware and protocols to use these indicators to capture relevant behavior. How can we ensure that the mix of indicators that we are using is optimal? Laboratories with the capacity for multiple assessments will be in the best position to provide information on the relative worth of the array of assessments.

Infrastructure

The necessary infrastructure to proceed with this research includes some of the items listed above such as high quality data, high quality assessments, and laboratories equipped for multiple assessments. Additionally, cyberinfrastructure with the capacity for large-scale data mining and aggregating multiple channels of information will be essential. Cyberinfrastructure will allow the collection of extremely detailed information on human behavior, innovative analyses of the information, and shared access to the resource.

Software comprises an important aspect of cyberinfrastructure and specific needs emerged over the course of the workshops, including data mining software, algorithms for combining different channels of information, and software for facial recognition, recognizing emotions and analyzing micro-expressions. Other useful items include software for data visualization, recognition of natural language, aggregating temporal information and machine learning.

Classified Research

The National Research Council suggested that the classified nature of some of the research in this area has prevented the accumulation of knowledge, and this concern was again raised in the workshops. Peer-reviewed research published in publicly available journals allows an accumulation of scientific knowledge as researchers check one another's approaches, findings, and interpretations. The current mix of public and classified research in these areas has the potential to hinder the building of scientific knowledge through independent confirmations of research findings and through the peer review process. The emphasis on openness needs to be balanced by concerns for security. It may be possible to create and maintain a

program that enables classified and unclassified research to be coordinated at the project level.

Additional Topics

A number of innovative topics were mentioned during the workshops that have the potential to inform research on physiological, psychological, and behavioral aspects of security evaluations. For example, there is emerging research on deception in non-human primates and research on the development of deception and understanding of deception in children. Analyses of trace elements in the human body, as well as DNA, may elucidate identity as well as geographic origins. The social psychology of terrorism provides a context for security considerations. In the long run, nanotechnology may provide the technology for continuous monitoring of cortisol stress hormones.

Workshop Summaries

Below is a summary of the major recommendations that resulted from each of the six workshops. More detailed information on individual workshops may be found in Appendices B-G.

Language and Deception

- Conduct well-controlled laboratory and field studies of the ways in which people alter their usage of words when deceiving vs. telling the truth.
- Develop new tools, including machine translation, voice transcription, and spectral analyses of voice quality, that explore natural word, phrase, and narrative use with applications for use in multiple languages.
- Develop a sizable and shareable corpus (in multiple languages) of empirically validated truthful and untruthful messages to test linguistic tools.

Behavioral Measures

- Determine the most elemental *physical and psychological* units of behavior that may suggest fear, stress or deception.
- Develop software and other tools for the gathering and analysis of the above.
- Investigate behavior at an *interpretive* level examining variables such as the immediacy, cognitive complexity, or plausibility of an account.
- Create necessary tools such as dictionaries of gestures and other culturally embedded behaviors for different cultural groups to provide a relevant comparative material.
- Develop and validate behavioral checklists across the variables of culture, personality, age, and gender, as well as variation in experience, education, language, and use of interpreters.

Emerging Technologies

- Devise new, and extend existing, algorithms for automated analysis of large databases, including visual data mining methods and link analysis.
- Expand tools for investigation of the social networks of those requesting security clearances.
- Establish the optimal technologies, policies, and procedures for electronic and manual storage and transfer of large databases of personal identity information.
- Continue the examination of the ethical and legal ramifications of data-mining, including the need to effectively characterize the difference between societal, political, and doctrinal representations of privacy.

Autonomic and Somatic Measures

- Assess and maximize the reliability, validity, and utility of pre-employment and periodic employment tests, including those that employ

polygraphy, particularly across cultures and variable contexts.

- Develop a database of field polygraph examinations that includes subject and examiner demographic information, case facts, test questions and polygraph charts to allow comparisons, generalizability studies, tests for gender and cultural effects and standardization of protocols and lab and test environments.

- Pursue new technologies such as laser Doppler vibrometery, eye tracker systems, radar, thermal imaging of facial blood flow, etc. that measure autonomic and physiological responses without direct contact.

Psychological Measures

- Adapt and adopt psychological assessments developed and evaluated for populations and purposes other than security contexts, e.g. mental health contexts.

- Facilitate psychological and sociological analyses of organizational factors that can inform security evaluations, e.g. structural features of organizations, vehicles for communication across and within departments, policies and procedures related to information sharing among employees and departments, and levels of employee autonomy.

- Develop a research-based taxonomy of deception (e.g., deception rooted in malevolence, self-protection, a desire to conceal, etc.) and the means to distinguish among the types.

- Gather cross-modal indices of deception linking psychological assessments to, e.g. autonomic nervous system indices.

- Extend and evaluate current tests of psychological status (e.g. implicit attitude, implicit cognition, empathy and unintentional racism) to expand the battery of tests aimed at detecting deception.

Functional Brain Imaging

- Evaluate the neural mechanisms that underlie the ability to intentionally suppress, distort, or fabricate information using cognitive neuroscience tools such as functional magnetic resonance imaging (fMRI).

- Correlate fMRI analyses of the neural signature of deception with physiological monitoring e.g. via the polygraph in real time studies.

- Investigate the ontogenetic development and maturation of an individual's skill at deceiving others. This should include investigation of the contextual and task dependencies of deceptive behavior.

- Pursue development of imaging tools that are portable and non-invasive, e.g. Near Infrared Spectroscopy (NIRS) and Near Infrared Imagery (NIRI), event related potential (ERP's), and the assessment of working memory.

Recommended Funding Mechanisms

Researchers and practitioners agreed on the following array of funding mechanisms, though there was no agreement on the optimal balance among the various potential investments. There was, however, agreement that single agency and interagency funding of multidisciplinary work could be particularly productive.

- Multidisciplinary centers with the scale, scope, and duration sufficient to address the big questions of these fields. Larger award size will allow for greater interdisciplinarity and provide resources for proof of concept experiments as well as the funding of risky-but-high-pay-off approaches. The longer duration will allow building a body of knowledge with subsequent studies built upon the findings of the earlier studies. Centers would benefit

from an explicit requirement to integrate research, training, and practice, including, for example, a significant graduate education component as well as embedded scholars and embedded practitioners. Centers could be co-located, distributed, or virtual. As for NSF funded centers, these would necessarily focus on the frontiers of knowledge at the intersection of disciplines and create a legacy of ideas, people, and promising new instrumentation.

- Individual investigator awards.

- Catalyst awards that bring together teams of researchers for developing programs of individual and joint research, and perhaps leading towards development of proposals for center-level support.

- Developmental workshops on issues including use of emerging technologies, legal/ethical issues, etc. Larger, multidisciplinary workshops may help potential colleagues identify one another.

- Rapid response funds (similar to the NSF-supported Small Grants for Exploratory Research; grants which can be reviewed and processed rapidly so as to investigate time-sensitive phenomena).

- Innovative collaborations between basic academic sciences and mission-oriented government funders.

- Training opportunities for undergraduate students, graduate students, and post doctoral fellows.

Summary Research Agenda

Research activities in the future that address the behavioral, psychological, and physiological aspects of security evaluations could be described as short-term and long-term and in some cases both short and long-term. Many of the major issues that emerged from the workshops, such as embedding researchers and practitioners, assessment instruments and protocols, infrastructure, scenarios, training and support, data issues, social/ethical/legal concerns, combining information, and research can be categorized as dealing with processes and protocols in security evaluation and are addressable in the short-term. Other issues, such as theoretical and empirical foundations, sensor development/encoding technology, closing the gap between science and practice, the societal implications of ineffective security evaluations, and understanding the roles of culture, gender, language, geography, acculturation, and individual differences will require greater time to fully develop, understand or achieve usable results. Due to the -nature of scientific research, it is easier to envision, plan for and predict short-term research than long-term research. Because long-term research is affected by new tools and insights, the nature of how science proceeds makes it difficult to predict such research needs and potentials very far into the future.

Short-term

Short-term research was defined as work that was likely to be accomplished within 5 years and reflected areas where there was a fairly large emerging literature. The areas of research that were most likely to yield near term research results were in the areas of behavior and language that may reflect security concerns. Development of data mining algorithms and software is quite advanced, though the linked privacy and confidentiality issues are in need of further research.

Longer-term

Long-term research was defined as work likely to take more than 5 years, and particularly in areas where there might currently be only a few publications. A longer-term research agenda is likely necessary in considering physiological and brain aspects of security evaluations and the use of psychological assessment.

Infrastructure

The most pressing needs for infrastructure that emerged through this process were needs for data and for protocols/test-beds/scenarios to be used in obtaining data. Standard scenarios could be developed fairly quickly. These data would include large data sets for comparison as well as data sets with real-life examples of deceit and truth. In addition, the cyberinfrastructure for data mining, aggregating multiple measures and analyzing complex physiological and neural activity were clearly needed.

Training

There is currently only a small body of researchers, scattered over a number of disciplines, conducting research directed at the goal of detecting deception. It is in the national interest to foster the development of an interdisciplinary "security science." This effort should provide opportunities for interaction between established practitioners and academic researchers while also providing for the future through mechanisms that attract and train junior scientists.

Classified Research

It was suggested that the disjuncture between the classified and unclassified work in this area was detrimental to building an emerging well-tested body of research, and to the extent possible, future research be unclassified.

Most Promising

Throughout the workshops, it was clear that combinations of information were most promising in detecting potential compromises of national security. This is codified in current security clearance procedures that combine polygraphy with interviews and analyses of public and private behavioral traces. New combinations and new approaches to combining information will move these fields forward.

Largely Neglected

The issues of countermeasures and their detection were not discussed much. Nor was there much discussion of the use of the web and data mining by criminal and terrorist activists -- these may be better topics for classified work, because they are not so much basic scientific questions as operational issues.

Innovative Approaches

Preliminary consideration of several innovative approaches was raised in the course of these workshops. For example, on the smallest scale, it was suggested that analyses of trace elements in the human body as well as molecular markers may elucidate identity as well as geographical origins. Nanotechnology may provide the technology for continuous monitoring of cortisol stress hormones. A focus on internal processes includes remote assessment of physiological indicators of stress, as well as assessment that may be linked with detection of critical micro-muscle movements.

A focus on behavior may lead to better understanding of deceptive processes through research on deception in non-human primates and the development of deception and the understanding of deception in children. What can we learn from individuals with autism, sociopaths, and others with mental health diagnoses? How can we use gaming as a research context? The social psychology of terrorism provides a context for security considerations. At a macro scale, remote sensing may track human movement and activity.

Also Essential

Serious consideration of issues of privacy and confidentiality as well as issues of cultural background are called for both as independent lines of work and as essential adjuncts to all the research.

Need for Collaborations and Coordination

The need for the work to be multidisciplinary was frequently mentioned, to the point that the development of a new scholarly field of security science was suggested. Also often mentioned were the need for scholars and practitioners to collaborate and the need for Federal agencies

to coordinate. The workshops indicated the need to bring together the many disciplines, the opportunity to generate rich data, and the challenging security problems in an iterative investigative process. Both "bottom-up" and "; top-down" research approaches and mechanisms are necessary. Bottom-up research will derive from practical considerations of data, while top-down research will evolve from understanding basic human processes.

Appendix A: Development and Funding of Workshops

In developing the structure of the workshops, the IAG identified scientists with recognized expertise in each workshop's focal area, selected one or more scientists as potential workshop leaders, and identified members of the user community with relevant expertise. The Behavioral and Cognitive Sciences Division of the NSF then solicited grant proposals from the recommended scientists. NSF workshop grants give the leader (PI) the intellectual freedom to create the agenda for the workshop and to select the invited participants. This is different from an NSF workshop that is conducted under a contract where NSF sets the agenda and selects the participants. These security valuation workshops were conducted as *grants*, not contracts. The summary plenary workshop and the draft report by MITRE were also funded as grants.

NSF conducted reviews of all grant proposals to assure that they met NSF merit review requirements, that the workshop would thoroughly address the topic, and that the additional crosscutting issues would be included. Each one and one-half day workshop was attended by approximately 20 individuals from the academic and operational/field communities who had relevant subject matter expertise and/or relevant operational experience. Members of the Interagency Advisory Committee, who represented the agencies identified in the Act, and other U.S. Government employees, were also invited to each workshop, largely as observers. The NSF grantees (PIs) maintained intellectual control over the selection of invited participants, organization of the workshop, and the exact topics to be covered.

Appendix B. Language and Deception in Security Evaluations (Workshop Report)

PI: Dr. James W. Pennebaker
University of Texas - Austin

Date: June 2-3, 2005

Workshop Goal:
The Language and Deception workshop focused on verbal and written behavior that may be linked to deception and present security risks.

A review of the literature indicates that there are multiple types of deception, such as lies of commission, omission, partial truths, and identity fraud. What is unclear is the degree to which different linguistic methods differ in their ability to detect these various forms of deception and how linguistic styles differ as a function of social situations, personality and psychological state. Workshop participants sought to better understand how language use is related to other presumed markers of deception, including changes in non-verbal behaviors and physiological activity. Similarly, they examined how theory-driven knowledge of the psychology of language could be integrated with the capabilities of natural language processing tools and measurement techniques?

Recent breakthroughs in computational linguistics, investigations of use and impact of the Internet, and fundamental social and psychological studies show that verbal cues are rich sources of information about people's thoughts, emotions, personality, intentions, motivations, and identity. Well-controlled laboratory studies, as well as field research, have found that people alter the ways they use words when deceiving vs. telling the truth. However, we do not yet know how language shifts across different aspects of deception.

Despite the fact that there are literally thousands of speech elements and acoustic features available for analysis, the number and variety of acoustic features examined in deception research have been extremely limited. As well, little use has been made of computational tools for classification and analysis. There is a need to develop new tools that explore natural word, phrase, and narrative use with applications for use in multiple languages. These tools should be validated across a wide range of contexts with existing data and deception relevant experiments. For example, can new tools enable us to determine whether there are reliable language shifts when a person is being deceptive about who they are versus what they did or know?

There is a pressing need for the development of a sizable and shareable corpus of empirically validated truthful and untruthful messages to test linguistic tools. This corpus should be collected from both controlled (laboratory) situations and applied (real world) settings, including known text samples from blogs, emails, natural conversations, interviews, phone calls, telephone text messages, instant messaging exchanges, chat rooms, written and spoken confessions, letters, criminal statements, hostage notes, and target group manifestos. The corpus should include text samples across multiple languages.

Promising Approaches include:

- Systematic empirical evaluation of detailed aspects of language, such as the relative distribution of function words and content words.
- Development of new technologies, including machine translation tools and voice transcription tools, that explore natural word, phrase, and narrative use across a wide range of contexts and languages, including real-time or near real-time text analyses.
- Use of promising natural language models that have emerged through computational linguistics for understanding truthful and deceptive speech.

- Analyses using voice quality and other spectral features, including the examination of speech phenomena, such as disfluencies and filled pauses.
- Computer-mediated communication (including e-mail, chat room, and instant messaging) that may provide unique and valuable opportunities to assess deception.
- Investigation of language clues as to personality, as well as individual characteristics, such as age and gender, and identity.
- Research as to the accuracy of *Statement Validity Analyses (SVA)*, particularly in field settings. SVA is a technique for assessing the truth of a statement based on the precept that truthful accounts of events differ significantly and noticeably from unfounded, falsified or distorted accounts. It is particularly difficult to establish a known error rate for field tests or to obtain comparison or control narratives for evaluation of critical statements.
- Utilization of large corpora of natural language text that can provide a comparison background for examining new language samples. These can build on existing resources, including identification of key languages that should be studied and for which language samples should be accumulated.
- Investigations to reduce the uncertainties relative to the effects of using a translator during an interview and the effects of conducting language analyses on translations.
- The study of individual differences in acquisition of new languages.
- Linguistic analyses including word, phrase, narrative, omission, commission, latencies, latent semantic analyses and prosody.

Appendix C. Behavioral Measures in Security Evaluations (Workshop Report)

PI: Mark Frank
State University of New York - Albany

Date: June 27-28, 2005

Workshop Goal:
The workshop on behavioral measures focused on observable behavior that may suggest deception or a security threat.

The workshop focused on the role people play in security threats, since it is people who plan and commit terrorist acts. The kinds of behaviors that are likely to pose security risks are context and culture dependent, and the contexts of concern are widely variable. For example, security screening may occur at a counter or checkpoint, via informal conversations, or via in-depth interviews. Assessments may be made informally and quickly, covertly or overtly, with or without consent, and be either brief or lengthy. Assessments frequently involve an interviewer and interviewee from different cultures. Even in the US context, the questioner and the person being questioned may be from different sub-cultures with different gestures, assumptions and behaviors. To provide a scientific analysis of behavioral assessments, that is, within controlled laboratory settings, the controlled setting must mimic the variables of concern that exist in the field as closely as possible. Yet this often is difficult because of limited access to subjects, restrictions imposed by Institutional Review Boards, and issues of ethics and privacy.

This workshop addressed such questions as: best approaches for interviewing suspects, witnesses, informants/assets, and hostile others. What happens physiologically and expressively when people are feeling emotions or thinking on their feet? How are these behaviors evidenced in a sit down interview, in an airport screening, and in public space settings? Workshop participants recognized how context affects the behaviors. Therefore, it is important to spend more time identifying best practices in interviewing techniques, and study of the effects of spatial arrangements, such as the use of space, chairs, and tables, to create an environment that allows the security personnel an opportunity to get the most accurate information possible.

Some studies involve investigating behavior at the most elemental *physical* units of measurement, such as logging the movements in the hands, feet, arms, legs, torso, head, eyebrows, lips, eyelids, or counting eye-blinks. Other efforts are aimed at measuring pupil dilation or the fundamental frequency, amplitude, and jitter of the voice, as well as tracking the number of words and pauses, response latency, or time spent talking. There is evidence that many emotions are cross-culturally universal, whereas gestures or other behaviors tend to be culturally specific. Identifying dictionaries of gesture or other culturally embedded behaviors for different cultural groups would provide a relevant comparison for studies of behavioral pattern analysis.

Other studies investigate behavior at the most elemental *psychological* level, which are often composites of the physical units described above. These behaviors have their own patterns, and there are empirical and conceptual reasons for examining them as distinct units. Some of these behavioral units include 1) manipulators or adaptors, which involve touching, rubbing, etc., of various body parts; 2) illustrators, that accompany speech to help keep the rhythm of the speech, emphasize a word, and show direction of thought; 3) emblems, which are gestures that have a speech equivalent, such as a head nod that indicates “yes”; 4) particular emotions represented in the facial expressions or expressed in the voice; and 5) other composite speech measures, such as speech rate and speech errors.

A third group of studies investigate behavior at an *interpretive* level, examining variables such as the immediacy, cognitive complexity, or plausibility of an account. These studies, which focus on

more abstract levels of judgment, are at the level at which untrained individuals show their best ability to judge deception. Even though there are these three groups of studies, there is a need to examine variables related to deception in a more interactive and integrated fashion, identifying patterns of agreement and contradiction.

The examination of facial expressions is one particularly promising area of investigation. Facial expressions can be biologically driven, involuntary and universal, as in the case of many emotions, or they can be socially learned voluntary expressions. With the assistance of automated facial movement software, studies are considering factors such as duration, smoothness, onset speed, and symmetry in distinguishing between the dynamic qualities of involuntary and voluntary expressions and smiles. These results have important applications for recognizing deception.

Combining synchronous, interrelated behavioral indicators through the integration of clues for a particular moment in time, rather than examining clues across time, is a novel approach that can identify discrepancies in the verbal/non-verbal performance of a subject of interest. The concept is based upon the study of expert polygraphers, who appear to have the ability to rapidly integrate and assess multiple lines of behavioral information. For example, if a person nods the head 'yes', but speaks the word 'no', then the emblem contradicts the spoken word. These contradictions then have become a much more reliable indicator of deception than simply the presence or absence of the emblem.

Promising Approaches include:

- Developing dictionaries of facial expression for cultures of interest.
- Developing symbolic gesture dictionaries for cultures of interest.
- Evaluating and validating, using both retrospective and prospective methodologies, behavioral check lists currently in use by security personnel and law enforcement, across the variables of culture, personality, age, and gender, as well as variation in experience, education, language, and use of interpreters.
- Understanding small signs of fear that may indicate security risk.
- Understanding external signs of internal states.
- Using behavior and gesture as cues to identity and nationality.
- Using gait and dress as clues.
- Linking behavioral checklists to the understanding of underlying processes.
- Tracking heads and hands may be an adequate proxy for more completely tracking behavior.

Appendix D. Emerging Technologies in Security Evaluations (Workshop Report)

PI: Dr. Lynette Hirschman and Dr. Gary Strong
MITRE Corporation

Date: July 13-14, 2005

Workshop Goal:
The emerging technologies workshop focused primarily on the use of data mining techniques for examining and aggregating extensive disjointed sources of data.

Massive amounts of textual data from communication and numeric records of many types contain important clues to national and homeland security threats; however, those data are often not organized and not amenable to analyses. The focus of the workshop on emerging technology was largely on data mining techniques and identity management technologies – approaches to look through large amounts of data for patterns and threats, as well as to mine pooled data for information on an individual.

Security evaluations require the collection of various kinds of data, primarily financial, criminal history, and other forms of "background data." Financial data are used to help determine whether or not (i) people have histories of meeting their financial obligations in a reliable and trustworthy manner, (ii) they are under excessive financial pressure that might make them more vulnerable to engage in inappropriate acts for money, and (iii) they have signs of unexplained affluence, which could be linked to payments for espionage or other criminal acts. Background data are used for a variety of purposes, including that of identity validation (i.e., to determine whether people are who they claim they are and that their references are genuine). However, the use of these data varies across agencies and adjudication practices. In addition, with the exception of continuing evaluation investigations being conducted by the Department of Defense, there is only limited use of automated analysis of databases that contain security-relevant information.

Workshop participants discussed the benefits that can be gained from investigation of the social networks of individuals requesting security clearances to determine if there are connections to known terrorists or criminals. However, there are also dangers of compromising individual civil rights against unwarranted search and seizure. The use of commercial (unregulated) databases for security evaluations may be perceived as threats to privacy, thereby discouraging workers from entering those parts of the Federal workforce that require security clearances. This application also may have untoward effects on international visitors (e.g., tourists, scientists and scholars, workers, and immigrants) whom we otherwise want to welcome to the U.S.

Promising Approaches include:

- Devising techniques for aggregating extensive, disjointed sources of data hold promise for extracting relevant information from very large data sets. These data mining techniques include, for example, relational data mining, social network analyses, visual data mining methods, link analysis and decision trees. Within each approach, the effect of various algorithms needs to be considered.
- Applying dynamic data mining structures which can take into account the identification of risk management across iterative data collections.
- Using historical and comparative data collected by security clearance agencies and including cases of compromise and abuse of access to privileged information in the past, data mining technologies should be applied to understanding the relations between security risks and the types data collected via (i) background investigations and (ii) routine access to law enforcement databases.

- Predicting how an individual's records-based "signature" will look in the years to come, and anticipate how to make this signature useful to security evaluations.
- Establishing the optimal technologies, policies, and procedures for electronic and manual storage and transfer of large databases of personal identity information.
- Identifying the structural, technological and social/cultural barriers to, and the cost-benefits of, government-to-government data sharing for the purpose of authenticating information.
- Investigating the possible impact of a "social auditing" infrastructure to serve a variety of homeland and national security interests, including national security evaluations; identity management; and insider threat assessment.
- Considering the extent to which Internet use promotes or facilitates hostile network behavior and investigating the best methods to identify, characterize and deter potential threats.
- Characterizing the difference between societal, political, and doctrinal representations of privacy so as to determine the meaning of privacy in each of these domains, and how flexible notions of privacy fluctuate over time and circumstances.
- Studying of the inhibitory /deterrent impact of data mining surveillance activity.

Appendix E. Autonomic and Somatic Measures in Security Evaluations (Workshop Report)

PI: Dr. John Kircher
University of Utah

Date: July 18-19, 2005

Workshop Goal:
The workshop focused on alternatives to the polygraph that are capable of assessing involuntary internal states associated with deceptive behavior.

The autonomic nervous system controls "involuntary" responses, including fight/flight responses to threat, danger and life threatening situations. Autonomic responses include heart rate, blood pressure, flushing, sweating, and respiration. Most intelligence and law enforcement agencies in the Federal government use measures of the autonomic nervous system and measures of skin response in security evaluations. Federal agencies routinely conduct polygraph examinations to screen applicants for employment and to conduct periodic tests of personnel with access to classified materials. Specific-incident polygraph tests also are used in criminal investigations to assess the veracity of suspects concerning their involvement in a specific criminal act. For both specific-incident and screening polygraphs, at least two types of questions are presented to the subject while electrodermal, cardiovascular, and respiration responses are recorded. Diagnoses of truth and deception are based on within-subject comparisons of the physiological responses to different types of test questions. Generally, lengthier and more consistent responses to specially prepared comparison questions, rather than to questions relating to the target issue, are considered indicative of deception. However, electrodermal, cardiovascular and respiration changes may reflect stress, arousal, attention and other affective experiences. As discussed in this workshop, significant breakthroughs in methods of detecting deception or hostile intent are unlikely to occur without a better understanding of the relationship of physiology and behavior to the cognitive and emotional processes that underlie stress and deception.

In 2003 the National Research Council reviewed the scientific literature on screening examinations. In their concluding report, they were critical of the polygraph in general, and especially critical of the screening polygraph, citing a weak theoretical basis, little empirical evidence of validity, and the lack of technological advancement in instrumentation. Since technological improvements would likely lead to only modest improvement in polygraph validity, the NRC recommended development of alternatives to the polygraph for security evaluations; however, they were admittedly unsure if any such alternative would improve upon the accuracy or utility of the screening polygraph.

Although screening and specific-incident polygraphs record the same physiological measures, there are differences in how the tests are structured and evaluated and the reasons for which they are administered. The likely base rate of deception also varies over testing contexts, and the validity of pre-employment screening and periodic tests appears to be lower than that established for specific-incident polygraphs. Despite the fact that there is a recognized need for more and better research on pre-employment and periodic use of the polygraph, such testing continues to be widely used by many agencies for access to the highest levels of security clearances.

The validity of the polygraph test across variable contexts and cultures remains largely unknown. This greatly limits the usefulness of the polygraph in pre-employment and periodic screening, as well as specific-incident test situations, for many Americans and other persons of interest. Additional research is needed to assess and maximize the reliability, validity, and utility of pre-employment and periodic employment tests. Moreover, a database of field polygraph examinations could be developed and made available to the scientific community. This database could include subject and examiner demographic information, case facts, test questions, polygraph charts and have the ability to be updated as new data and case facts, such as evidence admissions and

dispositions, become available. Such a database would allow for comparisons of test formats and scoring rules, generalizability studies, tests for gender and cultural effects and standardization of protocols and lab and test environments.

There are an increasing number of technologies being developed to measure autonomic and other physiologic responses other than those collected via the polygraph, many of which may co-vary with deception and/or behaviors that would pose security risks. Technologies that analyze voice stress and oculomotor activity are being tested in a variety of security and law enforcement contexts. In addition, there are new non-contact and remote technologies being developed, like laser Doppler vibrometery, eye tracker systems, radar, and artificial noses, that can measure many autonomic and physiological responses without the knowledge or consent of the individual. However, many of these technologies have not been developed within traditional scientific communities, where peer-review practices serve to establish acceptable levels of reliability and validity. There also are no standard behavioral assays, interview contexts or situations (e.g., pre-employment screening or criminal investigations) in which to evaluate these new and developing technologies.

Promising Approaches include:

- Large-scale and systematic, scientific research on the sensitivity, accuracy and validity of polygraph testing (including variations in pre- and post-interviews) across a variety of contexts and test subjects.
- Examination of electronic nose technology as a means of detecting body odors associated with fear that may be linked to security risks.
- Determination of the human skills that may optimize success of polygraphy.
- Investigation of acoustic properties of voice and voice stress for use in assessing credibility, deception, or hostile intent. A database of test samples of audio recordings of known truthfulness to identify diagnostic aspects of voice and for use in independently evaluating voice stress analysis technologies.
- Measurement of facial blood flow that may indicate underlying emotional arousal can be assessed at a distance with non-contact thermal imaging.
- Investigation of combinations of autonomic nervous system data or measures from multiple channels that have the potential to significantly increase the accuracy of assessments of stress that may be linked to security risks.
- Determination of the effects of culture, personality, age, gender, experience, education, language, and the use of interpreters on the autonomic measures taken in polygraph testing and on the recommendations based on polygraph tests.
- Investigation of the efficacy of various countermeasures, counter-countermeasures, and countermeasure detection on the autonomic measures taken in polygraph testing, and the relationship between traditional polygraph measures and measures employing newer technologies.
- Investigation of emerging technologies for the assessment of stress or hostile intent, including remote electrodermal and vibrometric measurements, especially those using Laser-Doppler and radar technology, of arterial pulse pressure waveforms, respiration, and muscle contractions that can allow sophisticated assessment at a distance.
- Investigation of oculomotor responses that are promising indices of deception and wariness that can be assessed at a distance. Robust remote eye tracker systems could be used in the field for source verification, perpetrator identification, witness corroboration, and detection of concealed information.

Appendix F. Psychological Measures in Security Evaluations (Workshop Report)

PI: Dr. James Breckenridge
Stanford University

Date: July 25-26, 2005

Workshop Goal:
The workshop on psychological assessments considered tests, training, insider and outsider threat, workplace climate, and specific research needs.

Psychological assessments that are used within intelligence and other national security agencies typically have been developed and evaluated for populations and purposes other than security contexts. Many assessments derive from a mental health framework. Commercially developed measures commonly lack sufficiently documented validation for their purported applications. Therefore, security agencies may be seriously misinformed about persons of interest. This misinformation, far from being neutral, may have profoundly deleterious effects, in part because valuable resources may be assigned to marginally relevant investigations, thereby compromising the national security effort.

Creating a secure workforce can be facilitated by how the workplace is organized and managed. Psychological and sociological analyses of organizational structure and worker performance has shown that employee performance depends largely on organizational factors, such as the structure of the organization, vehicles for communication across and within departments, policies and procedures related to information sharing among employees and departments, and the extent to which employees are given autonomy to perform their job tasks. For example, directive and top-down communications have been shown to promote organizational cultures that neglect the importance of information sharing, and competitiveness and distrust evolve from conditions where information is not shared among and between managers and employees.

Organization and management theory suggest another approach to ensure a secure workforce: Rather than employing a reactive strategy – where the U.S. Government responds to security breaks that have already happened – a proactive strategy may serve to create secure organizations in ways that promote employee cooperation. This should be considered as an alternative model for dealing with both "outsider" and "insider threat" security risks. Security evaluation concerns relevant to employment should not be considered as separate from organizational structure and its impact on employee behavior.

Deceptive behavior may be rooted in a variety of motivations: malevolence, self-protection, a desire to conceal and so forth. It is critical to develop a taxonomy of deception and the means to distinguish between the types if, as been hypothesized, they produce distinctive neurological and physiological signatures. It is also important to distinguish between personality types that are likely characterized by different neurological and physiological signatures in response to interrogation techniques.

Psychological and personality assessments serve to add another dimension to the neurological, behavioral, and physiological signatures of deception. Identifying underlying mechanisms of deception in this way will enhance our ability to select the most prominent peripheral indices of deception for ready and noninvasive testing in a variety of settings, from the clinical to the interrogative. It will further enable characterization of individual variation in these indices based on personality types due to the likely differences across groups in responses to deception. Detection methods often involve inducement of stress responses that vary considerably by personality traits.

The workshop on psychological measures also addressed issues of interrogation, including discussion of the false information that may be elicited with harsh interrogation. Alternatives were explored that were based on influence/motivational approaches, including strategies of appealing to motivations such as belongingness, reciprocity, and the need to reduce cognitive dissonance.

Psychological assessment in security settings can be severely limited by a strong reliance on self-reports of critical data. Individuals may report erroneous or even intentionally deceptive information because they seek to present themselves in a manner they deem desirable to the examiner or because they wish to conceal personal vulnerabilities or other sensitive information. False memories may be perceived as real. Individuals' reports also may be distorted by educational deficits or by cultural restraints that discourage candid disclosure of private experience.

Promising Approaches include:

- Measuring the affect experienced while completing questionnaires with autonomic nervous system indices and eye tracking.
- Using reaction time and keystrokes measures during psychological assessments to give ongoing assessment of affect.
- Adapting current tests of implicit attitude, implicit cognition, empathy and unintentional racism to create a battery of tests aimed at detecting deception.
- Adapting psychological tests and measures developed for mental health assessment for use in security evaluation settings.
- Developing cultural competency training evaluations for personnel responsible for face-to-face interaction with foreign nationals, as well as cultural groups and sub-groups in the United States.
- Developing a widespread understanding by all those involved at all levels of the parameters of effective assessments, including reliability, validity, sensitivity and specificity.
- Comparing neurological differences between psychopaths and normal individuals to improve understanding of the neural processes related to deception.

Appendix G. Functional Brain Imaging in Security Evaluations (Workshop Report)

PI: Dr. Thomas Zeffiro
Georgetown University

Date: August 1-2, 2005

Workshop Goal:
The workshop on functional brain imaging focused on the neural mechanisms that underlie the ability to intentionally suppress, distort, or fabricate information and the ability to visualize these mechanisms.

The neural mechanisms that underlie the ability to intentionally suppress, distort, or fabricate information are not yet well understood. Clues about the neural basis of deception have been found using neuropsychological approaches. There are a number of research efforts underway to gain such understanding, and a handful of papers reporting research results using cognitive neuroscience methods such as functional magnetic resonance imaging (fMRI) have been published. These efforts have identified a set of candidate neural subsystems as being potentially involved in the generation of deception. However, the relation between the imaging data and behavior is not well understood. A detailed understanding of the neural basis of deception could be used to develop new approaches to detecting deception based on functional neuroimaging methods, as well as to address the broader question of the relationship between brain activity and behavior.

Understanding the neural mechanisms involved in deception, and using neural signals to detect deception, depends on further advances not only in neuroimaging but also in investigations of the behavioral, psychological and other physiological aspects of deceptive behavior, and in discovery of the principles of brain mechanisms as they relate to behavior. The research in this area is in its beginning stages.

An individual's skill at deceiving another is not present at birth, but develops along an unknown time course through the normal course of brain and psychological maturation. Contextual and task dependencies are not yet understood. These complexities of deception make it difficult to gain a deep understanding of the neural mechanisms corresponding to deceptive behavior or intent. Brain imaging techniques are likely to be fruitful but there is still much that is unknown.

The primary goal of this workshop was to explore fully the application of functional brain imaging to the covert mental process of deception and to directly advance discovery and understanding while promoting teaching, training, and learning. The presentations made by principal researchers synthesized the leading edge of knowledge in numerous important domains, including methodologies for functional brain imaging; empirical results of functional brain imaging studies of basic, cognitive processes, such as memory, attention, emotion, and imagery; and empirical results of brain imaging studies of "more esoteric" processes. Also discussed were critical analyses of brain imaging approaches, including challenges to ecological validity and participant demand characteristics; synthesis of individual and group variation in brain imaging studies, as well as behavioral studies of deception; and, most importantly, generation of research projects applying sophisticated brain imaging techniques to the study of the complex phenomenon of deception.

Although fMRI has shown promise as a tool in understanding and recognizing the neuropsychological processes of deception, researchers are working to better understand the relative importance of variation within individuals and between individuals. Researchers are correlating fMRI analyses of the neural signature of deception with physiological monitoring via the polygraph in real time studies. Also fMRI's limitations on mobility and portability are pushing the development of new non-invasive and portable imaging devices like Near Infrared Spectroscopy

(NIRS) and Near Infrared Imagery (NIRI), event-related potential (ERP's), and the assessment of working memory.

Promising Approaches include:

- Application of current state-of-the-art brain imaging methodologies to analyses of brain activities that correspond to putative deceptive behavior, using instances of deception that are best suited for investigation using functional neuroimaging.
- Development of ways to conduct brain-imaging studies without requiring an overt response from research participants, while still ensuring participant accountability.
- Development of realistic scenarios to examine "deceptive behaviors" that can be analyzed with current fMRI technologies, including social behaviors.
- Integration of analyses of deception with neuroimaging-based investigations of memory, attention, emotion, and mental imagery, and other complex psychological and behavioral phenomena.
- Assessment of Central Nervous System responses during deception that may be influenced by drugs, cultural differences, age, and even by intelligence.
- Investigation of deception as a risk taking activity, with "low stakes" and "high stakes" risks.

Appendix H. Summary of Federally Funded Research

A wide range of Federally funded research pertinent to the conduct of individual security evaluations has been undertaken in the last decade. Agencies supporting research in this arena include the Department of Defense (DoD), Department of Energy (DOE), Department of Justice (DoJ), Department of Homeland Security (DHS), National Institutes of Health (NIH), and the National Science Foundation (NSF). The Department of Energy and the Department of Defense's Polygraph Institute (DoDPI) and Defense Personnel Security Research Center (PERSEREC) have been the most active in proposing and supporting the testing, development, and improvement of protocols and methods related to the polygraph interview and background screening investigations. In addition, efforts are underway to develop practical, novel approaches to evaluating security threats and detecting deception. Paralleling the development of new methods has been the development of new systems to recognize the use of countermeasures during polygraph interviews. Below are summaries of recently completed or initiated unclassified research that was collected in the context of these workshops.

Federal agencies with closer ties to field needs and operational communities, as well as a history of mission-specific research, are conducting applied research and product development; these include Department of Defense, Department of Energy, Department of Homeland Security, National Institutes of Health and National Institute of Justice for the support of applied research in the behavioral, psychological and physiological sciences relevant to security evaluations. In addition to basic and applied research, research addressing ethical and privacy issues related to the implementation of methods and tools to assess individuals for security risks is essential. Further research that addresses multi-cultural and cross-cultural challenges related to security evaluation would also be available.

The identification of physiological measures along with verbal, behavioral, and cultural cues for deception has seen the greatest focus in unclassified Federal research funding. In particular, a number of agencies have been active in the development of techniques, tools, and sensors for rapidly assessing potentially deceptive individuals. Determining the specific and most sensitive physiological features relevant to truth or deception discrimination and the relationship between those features is progressing rapidly. DoDPI and DOE have been leaders in supporting research on non-contact and remote technologies, such as laser Doppler vibrometry, thermal and infrared image analysis of the face and skin surface. These technologies are being tested and developed to detect stress, emotion, and physiological functions, like heart rate, muscle tension, blood pressure, and respiration rate. Technological improvements have led to a greater degree of sensitivity in measures of facial skin temperatures and reactivity.

For example, support from DoE for research has developed Micropower Image Radar, a non-contact sensor that detects minute motions to recognize and assess micro-facial expressions and monitor physiological measures like heart palpitations and blood surge as signatures of relevant physiological or emotional states. Electronic noses are being improved to identify and detect key effluent or skin chemical markers associated with stress, while systems that monitor eye movements for evidence of prior knowledge and recognition are being developed and tested.

In an effort to assess effectiveness and to improve the currently available polygraph technology, researchers have found the measure of Pulse Transit Time to be a sensitive alternative cardiographic measure. Other reconsiderations of cardiographic measures have investigated the relevance of factors such as race, finding no significant difference.

A number of neuroscientists working with DoDPI, NSF, and NIH are conducting research to examine measures of vascular physiology related to mental stress and establishing the neurobiological correlates of deception using fMRI brain imaging. At the same time, researchers at the DoE are working to develop tools to detect brain wave patterns associated with stress-related activities. Likewise, NSF supported research is showing Diffuse Optical Imaging to be a promising

new technology that may be useful as a portable, less expensive alternative to fMRI in the detection of neural processes. In related work, NIH investigators are looking at the neuropsychology of primate social cognition to aid in understanding the basic underpinnings of psychiatric, degenerative and developmental disorders that affect facial recognition and emotional processing.

Researchers at DoD Center for the Advanced Study of Language, Defense Advanced Research Projects Agency (DARPA) and DHS are working to establish baseline behavioral and verbal/non-verbal and linguistic cues against which later behavioral mannerism can be evaluated. For example, more visible actions, motions, and gestures are also being studied to determine behavioral cues of deception. Likewise, psychologists, with NIH support, are studying the cross-cultural context of lying, the acquisition of the concept of lying, and the micro and macro-environmental effects on moral conceptions of lying to better understand the role, perceptions, and development of lying by individuals with various cultural, social, and economic backgrounds.

To efficiently analyze and integrate the massive amounts of data created in the security evaluation process, computer scientists are developing computer assisted decision-making systems and algorithms to aid in assessment of polygraph screening results and the evaluation of diagnostics of deception. Other DoDPI researchers are conducting comparative analyses of the polygraph with other screening and diagnostic tools to assess and improve their validity and reliability. DoDPI supported research has been testing and refining the polygraph interview protocol, specifically the relationship of question pairing, the number of questions in a series and the relative order of the questions.

In the linguistic arena of security related research, voice stress analysis and speech characteristics, like pitch, hesitation, content, and speech errors, are providing significant advances. NSF scientists are experimenting with automatic speaker recognition systems to identify stylistic features of speech that indicate complex behaviors and emotions. Additional linguistic research is evaluating and validating methods and techniques of detecting deception by verbal analyses through comparisons to biodata, integrity tests, polygraph results, and records of past behavior. Language scientists are assessing the necessary minimum or summary levels of translation versus verbatim foreign language translation in intelligence analyses, and analysts are being aided by the NIJ supported development of a number of foreign language speech translation technologies.

The development of new data mining technologies has been one of the greatest areas of attention in security evaluation research and development in terms of volume of data, levels of integration, and breadth of research across government funding agencies. Specifically, agencies like the Department of Defense's Advanced Research and Development Activity (ARDA) and PERSEREC, along with DOE and NSF, are developing better tools and data mining algorithms to integrate and analyze patterns, anomalies, and regularities in massive sets of motion-time-series data. NSF-funded researchers are assembling automated systems for video indexing and content analysis that include person and text detection. Accompanying better data mining technologies is research that examines the analytical processes of analysts. The outcome of this track will better equip analysts with pertinent data, while allowing them to work through biases and assumptions that may hinder the development and recognition of novel intelligence.

While noting that this summary only includes non-classified research, this overview demonstrates that relevant Federal agencies are currently supporting or conducting complementary basic and applied research that will enhance the ability to detect deception and further the agencies' goals.

United States District Court for The District of Columbia

Eric Croddy *Et Al.*, Plaintiffs, v.
Federal Bureau of Investigation *Et Al.*, Defendants

Civil Action No. 00-651 (EGS)

Memorandum Opinion

Plaintiffs bring this action raising numerous claims in connection with their non-selection for employment by Defendants, the Federal Bureau of Investigation ("FBI") and the United States Secret Service ("Secret Service"). Specifically, Plaintiffs allege that they applied for employment with Defendants, that as part of the application process they were required to take a polygraph examination, and that as a result of that examination they were not offered employment. They contend that the polygraph testing is unreliable, that their "false positives" improperly served as the basis to deny them employment with these agencies, and these results affect their potential employment with other law enforcement agencies. Plaintiffs claim that the use of polygraph examinations in the application process violates the Administrative Procedure Act, 5 U.S.C. § 701 *et seq.,* the Fifth Amendment, and the Constitutional right to privacy.

Pending before the Court are Plaintiffs' motion for summary judgment, and Defendants' motion to dismiss in part and for summary judgment. Upon consideration of the parties' motions, the responses and replies thereto, and the entire record, the Court determines that Plaintiffs' constitutional claims fail on the merits, and that their administrative claims are either barred for lack of jurisdiction, or fail on the merits. Therefore, for the reasons stated herein, Plaintiffs' motion is **DENIED,** and Defendants' motion is **GRANTED.**

Background[i]

The FBI conducts polygraph examinations of applicants for employment to the FBI. [ii] DMF at 1. Plaintiff Brian Weiler ("Weiler") applied for the position of Special Agent with the FBI in 1997, and underwent a polygraph examination in December 1999. DMF at 3. Weiler did not pass the polygraph examination and his request for a second examination was denied. DMF at 3. Plaintiff Susan Wright ("Wright") applied for the position of physical scientist forensic examiner with the FBI, and underwent a polygraph examination in November 1999. DMF at 3-4. Wright did not pass the polygraph examination and her request for a second examination was denied. DMF at 4-5. The FBI rejected Weiler and Wright's applications for employment because they failed the polygraph examinations. DMF at 4; D's response at 4 n.3.

The Secret Service conducts polygraph examinations of applicants for employment for the position of Special Agent. DMF at 5. Applicants cannot proceed in the application process unless they pass the polygraph examination. DMF at 6. Plaintiff William Roche ("Roche") applied for the position of Special Agent with the Secret Service in 1999. DMF at 7. Roche did not pass two polygraph examinations and was not selected for employment as a Secret Agent. DMF at 7-8. Roche never applied for another law enforcement position after failing the Secret Service polygraph examination. DMF at 8.

Plaintiff Darryn Mitchell Moore ("Moore") applied for the position of Special Agent with the Secret Service in 1988. DMF at 9. Moore did not pass two polygraph examinations and was not selected for employment as a Special Agent. DMF at 9. Moore voluntarily left a law enforcement job with the Atlanta Police Department to pursue journalism, his educational major. DMF at 10.

Plaintiff Thomas Miller ("Miller")

applied for the position of Special Agent with the Secret Service in 1994. DMF at 10. Miller did not pass two polygraph examinations and was not selected for employment as a Special Agent. DMF at 10-11. As of December 2003, Miller was working as a Special Agent with the Immigration and Customs Enforcement Agency, a law enforcement position within the Department of Homeland Security ("DHS"). DMF at 11.

Plaintiff Eileen Moynahan ("Moynahan") applied for a position of Special Agent with the Secret Service in 1993. DMF at 11. Moynahan did not pass three polygraph examinations and was not selected for employment as a Special Agent. DMF at 1112. As of September 2003, Moynahan was working for the Drug Enforcement Agency ("DEA") as an intelligence research specialist, which is a law enforcement position. DMF at 12. Moynahan was hired in this position after disclosing to the DEA that she had failed the Secret Service's polygraph examination. DMF at 12-13.

Analysis

Plaintiffs have brought three claims in this suit, alleging that: (1) Defendants' dissemination of the information that Plaintiffs failed polygraph examinations deprives them of their occupational and reputation-based liberty interests without due process; (2) Defendants violated their constitutional right to privacy because they asked questions regarding their medical, psychological, sexual, criminal, and drug use histories during the examinations; and (3) Defendants' use of the polygraph examination in the employment process violates the APA. Both parties seek summary judgment on all the claims. In addition, Defendants ask the Court to dismiss the non-constitutional claims for lack of jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1).

I. Standard of Review

A motion under Rule 12(b)(1) presents a threshold challenge to the Court's jurisdiction. *Haase v. Sessions,* 835 F.2d 902, 906 (D.C. Cir. 1987). The Court may resolve a Rule 12(b)(1) motion based solely on the complaint, or if necessary, may look beyond the allegations of the complaint to affidavits and other extrinsic information to determine the existence of jurisdiction. *See id.* at 908; *Herbert v.* Nat'l *Acad. of Sci.,* 974 F.2d 192, 197 (D.C. Cir. 1992). The Court must accept as true all the factual allegations contained in the complaint, but the plaintiff bears the burden of proving jurisdiction by a preponderance of the evidence. *Bennett v. Ridge,* 321 F. Supp. 2d 49, 51-52 (D.D.C. 2004).

Summary judgment should be granted only if the moving party has shown that there are no genuine issues of material fact and that the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56; *Celotex Corp. v. Catrett,* 477 U.S. 317, 322 (1986); *Waterhouse v. District of Columbia,* 298 F.3d 989, 991 (D.C. Cir. 2002). In determining whether a genuine issue of material fact exists, the Court must view all facts in the light most favorable to the non-moving party. *See Matsushita Elec. Indus. Co. v. Zenith Radio Corp.,* 475 U.S. 574, 587 (1986). The non-moving party's opposition, however, must consist of more than mere unsupported allegations or denials and must be supported by affidavits or other competent evidence setting forth specific facts showing that there is a genuine issue for trial. Fed. R. Civ. P. 56(e); *see Celotex Corp.,* 477 U.S. at 324.

II. Due Process Claims

Plaintiffs claim that Defendants have damaged their reputations and occupational prospects without due process of law by disseminating the defamatory results of their polygraph examinations. In particular, they claim that Defendants have published their findings that Plaintiffs failed polygraph examinations, and thus injured Plaintiffs' job prospects with other federal law enforcement agencies.

In order to establish a violation of procedural due process, Plaintiffs must show that they were deprived of a constitutionally protected interest. *See Graham v. DOJ,* 2002 WL 32511002, at *4 (D.D.C. 2002). A claim for deprivation of a liberty interest based on the defamatory statements of government officials in combination with an adverse employment

action may proceed on one of two theories. *See Holman v. Williams,* 436 F. Supp. 2d 68, 78 (D.D.C. 2006). The two theories are referred to as "reputation-plus" and "stigma or disability." *See id.* at 78-79.

Under the "reputation-plus" theory, an employee's liberty interest is infringed when there is "official defamation" accompanied by either a "discharge from government employment *or at least a demotion in rank or pay." O'Donnell v. Barry,* 148 F.3d 1126, 1140 (D.C. Cir. 1998). Plaintiffs' claims do not satisfy either prong of the "reputation-plus" standard. Government-disseminated information must be false in order to be considered defamatory. *See Graham,* 2002 WL 32511002, at *4 n.2 (holding that a letter was not defamatory because its contents were not false); *see also Codd v. Velger,* 429 U.S. 624, 628 (1977) (holding that no hearing was required because plaintiff did not allege that government's report was false). Though reports that Plaintiffs failed polygraph examinations may imply that they lied or had used drugs, the reports are technically accurate – there is no dispute that Plaintiffs did in fact fail the Defendants' examinations. Therefore, information about Plaintiffs' polygraph results do not constitute defamation. *See Graham,* 2002 WL 32511002, at *4 n.2.

In addition, Plaintiffs fail the second prong of the "reputation-plus" standard because they were neither discharged nor demoted – they were merely not offered a position. *See O'Donnell, 148* F.3d at *1140.* [iii] The D.C. Circuit has explained that a discharge or demotion is required to ensure that the damage to the employee's reputation is sufficiently severe, and to limit the scope of permissible due process claims. *See id.* Even accepting Plaintiffs' characterization of Defendants' actions as revoking conditional offers of employment, those actions constitute neither a discharge nor demotion from an employment position. Therefore, Plaintiffs have not demonstrated the loss of a liberty interest under the "reputation-plus" theory.

Under the second liberty interest theory, deemed "stigma or disability," a plaintiff's liberty interest is infringed when there is an "adverse employment action and a stigma or other disability" that forecloses the plaintiff's freedom to take advantage of other employment opportunities. *Id.; Holman,* 436 F. Supp. 2d at 79. [iv] The government action and stigma must "seriously affect[], if not destroy[]" the plaintiff's ability to pursue her chosen profession. *O'Donnell,* 148 F.3d at 1141 (quoting *Kartseva v. State Dep't,* 37 F.3d 1524, 1529 (D.C. Cir. 1995)). A plaintiff's job prospects are sufficiently damaged if the official action either automatically bars the plaintiff from a range of government positions, or generally blocks her from pursuing employment in her chosen field of interest. *Holman,* 436 F. Supp. 2d at 79.

In this case, Plaintiffs concede that they have no evidence that Defendants disseminated their polygraph results, or that they were denied any job, other than with the Defendants, because of their polygraph examinations. *See* Pls.' Reply to Opp'n to Pls.' Mot. for Summ. J. at 4-5. In fact, Miller and Moynahan attained law enforcement positions with the DHS and DEA respectively, notwithstanding their failed polygraph examinations. Plaintiffs invite the Court to speculate that publication of their polygraph results will necessarily lead to the elimination of otherwise available job opportunities. The Court, however, has no basis for doing so. [v] Just as the FBI and Secret Service do not conclusively rely on the polygraph results of other agencies, [vi] other agencies may not rely on Defendants' results. Absent any evidence that Defendants' actions have foreclosed Plaintiffs' other job opportunities, Plaintiffs have not demonstrated the loss of a liberty interest under the "stigma or disability" theory. *See Graham,* 2002 WL 32511002, at *5.

Because Plaintiffs have not shown that Defendants deprived them of a protected liberty interest, their procedural due process claims fail as a matter of law.

III. Constitutional Right to Privacy

Plaintiffs claim that Defendants violated their constitutional right to privacy because they asked Plaintiffs questions regarding their medical, psychological, sexual, criminal, and drug use histories during their polygraph examinations. In particular, Plaintiffs challenge the Secret Service's

practice of asking applicants whether they had committed adultery and other sexual crimes.[vii]

The D.C. Circuit has expressed grave doubts as to whether there is a Constitutional right protecting the disclosure of confidential information. *See Am. Fed'n of Gov't Employees v.*

HUD, 118 F.3d 786, 791 (D.C. Cir. 1997). The court, however, has not directly resolved the question. *See id.* at 793. Instead, in that case, the court held that even assuming the right exists, it was not violated by the employee questionnaires utilized by the Department of Housing and Development ("HUD") and the Department of Defense ("DOD"). *See id.* at 793-95. The court held that HUD could legitimately inquire into their potential employees' drug use and financial troubles because they would be in positions of public trust. *Id.* at 794 ("When presented with a reasonable determination we are reluctant to second-guess the agencies' conclusions."). The court was even more reluctant to reject the DOD procedures because they concerned national defense and security, and approved questions regarding the employees' mental health and expunged criminal history. *See id.*

In this case, Plaintiffs were applying for positions of public trust concerning the security of the nation and of our elected officials. Therefore, even assuming there exists a constitutional right to non-disclosure of private information, Defendants can legitimately inquire into the applicants' financial, drug use, health, and criminal history. *See id.* at 793-94. [viii] With regard to the Secret Service's specific questions, the agency has made a reasonable determination that there is a danger if its employees in sensitive positions could be blackmailed for some reason. The Court will not second-guess that conclusion, and therefore the agency can legitimately ask whether applicants committed adultery or serious crimes. *See id.* at 793. Accordingly, the Court rejects Plaintiffs' constitutional privacy claims as a matter of law.

IV. APA Claims

Plaintiffs claim that Defendants' use of polygraph examinations violates the APA. In particular, they argue first that Defendants violated their own regulations in denying employment solely on the basis of failed polygraph examinations. Second, they argue that Defendants' practice of denying employment solely on the basis of failed polygraph examinations is arbitrary and capricious.

The APA provides for judicial review of a "final agency action for which there is no other adequate remedy in a court," 5 U.S.C. § 704, and allows for judicial review "except to the extent that . . . (1) statutes preclude judicial review; or (2) agency action is committed to agency discretion by law," 5 U.S.C. § 701(a). *Mistick PBT v. Chao,* 440 F.3d 503, 509 (D.C. Cir. 2006). Defendants argue that relief under the APA is unavailable for several reasons: (1) the Civil Service Reform Act of 1978 ("CSRA") and Privacy Act preclude APA review; (2) the actions at issue are committed to agency discretion by law; and (3) the APA claims fail on the merits.

A. Preclusion of APA Claims by Other Statutes

The CSRA is a comprehensive statute that prescribes protections and remedies for federal civil servants. *See Graham v. DOJ,* 2002 WL 32511002, at *2 (D.D.C. 2002). It is well-settled that the CSRA precludes all other claims challenging federal personnel actions, included APA claims. *Id.* Even if the CSRA does not provide a remedy for a particular federal employee, the CSRA still precludes personnel-based APA claims because that means the contested action is committed to agency discretion by law. *See id.* at *2-3. Therefore, the fact that the FBI is generally exempted from the CSRA's scheme does not diminish the scope of the CSRA's preclusive effect. *See id.* at *2; 5 U.S.C. § 2302(a)(2)(C)(ii); *Graham v. Ashcroft,* 358 F.3d 931, 934-35 (D.C. Cir. 2004) (holding that employees' personnel claims are still precluded even if the CSRA does not provide a remedy for a particular type of personnel action). This preclusion remains in effect even for claims that an agency has violated its own regulations. *See Graham,* 358 F.3d at 935.

Therefore, the determinative question is whether Plaintiffs' APA claims fall within the

purview of the CSRA. [ix] Applicants for federal employment are also covered by the CSRA. *See Spagnola v. Mathis,* 859 F.2d. 223, 225 n.3 (D.C. Cir. 1988) (per curiam). The "prohibited personnel practices" Congress included in the CSRA remedial scheme are set forth at 5 U.S.C. § 2302. *Id.* at 225. The definition sweeps broadly to address the "tak[ing] or fail[ure] to take any . . . personnel action if the taking or failure to take such action violates any law, rule, or regulation implementing, or directly concerning, the merit system principles contained in section 2301 of this title." *Id.;* 5 U.S.C. § 2302(b)(11). One such merit principle provides: "All employees and applicants for employment should receive fair and equitable treatment in all aspects of personnel management." § 2301(b)(2). Plaintiffs' claim that Defendants' reliance on polygraph results is arbitrary, or that the polygraph process is somehow unfair, directly implicates this principle, and therefore would be considered a prohibited personnel practice. *See Spagnola,* 859 F.2d. at 225 n.3. Plaintiffs' APA claims thus fall within the ambit of the CSRA, and are therefore precluded.[x]

B. Whether Actions are Committed to Agency Discretion

Were Plaintiffs' APA claims not precluded by the CSRA, they are still barred in part because they challenge actions committed to agency discretion. *See 5* U.S.C. § 701(a)(2). FBI hiring decisions, in particular, have been held unreviewable under the APA because they are an exercise of agency discretion, and there is no meaningful statutory standard against which to judge the FBI's exercise of discretion. *See Padula v. Webster,* 822 F.2d 97, 100 (D.C. Cir. 1987); 5 U.S.C. § 2302(a)(2)(C)(ii) (exempting FBI from CSRA). Secret Service hiring decisions are similarly an exercise of agency discretion, and Plaintiffs have provided no statutory standard by which this Court can evaluate those decisions. Therefore, Plaintiffs' claims that Defendants' use of polygraph examinations is arbitrary and capricious cannot be brought under the APA. *See Heckler v. Chaney,* 470 U.S. 821, 830 (1985) (holding that if Congress has not provided standards to judge an agency's discretion, it is unreviewable under 5 U.S.C. § 701(a)(2)).

Plaintiffs' APA claims that Defendants violated their own regulations, however, may still be considered. "It is well settled that an agency, even one that enjoys broad discretion, must adhere to voluntarily adopted, binding policies that limit its discretion." *Padula,* 822 F.2d at 100. Therefore, Plaintiffs' APA claims based on regulations are not barred by 5 U.S.C. § 701(a)(2). *See id.* at 100-01.

C. Whether Defendants Violated Regulations

Plaintiffs challenge Defendants' policies of denying employment solely on the basis of failed polygraph exams.

Plaintiffs argue that Defendants' policies violate the instructions of DOD's Polygraph Institute ("DODPI"), and the FBI's Manual of Investigative Operations and Guidelines ("MIOG"). The DODPI instructions do not bar Defendants' policies, however, because they apply only to DOD, and are not binding on any other agencies. *See* Defs.' Ex. 23 at 55, 69-71 (deposition of William Norris). Plaintiffs cite no authority to show that the DODPI instructions are binding on Defendants. Therefore, Plaintiffs' claims based on the DODPI instructions fail as a matter of law.

Plaintiffs argue that the FBI's hiring policy contravenes several provisions of the MIOG. [xi] The first, § 13-22.2(2) states that "[p]olygraph results are not to be relied upon to the exclusion of other evidence or knowledge obtained during the course of a complete investigation." The second, § 13-22.5, states that "[u]se of polygraph will in no way absolve Agents of their responsibility to conduct all logical investigation possible by conventional means in order to verify the truthfulness and accuracy of information furnished." The third, § 13-22.12(5) states that a "preemployment polygraph examination is one element of the overall applicant screening process [and] is not to be considered as a substitute for a thorough and complete background investigation."

The first and second provisions cited by Plaintiffs refer to the use of polygraphs in general criminal investigations, and not specifically to the hiring process. *See §* 13-22.2(2) ("The following general policies apply to

the use of the polygraph by the FBI."). In contrast, § 13-22.12 specifically covers polygraph examinations of FBI applicants. While § 13-22.12(5) does state that the polygraph examination is only part of the screening process, the FBI's policy does not violate that provision. Had Plaintiffs passed the polygraph examination, they still would have been subject to a complete background examination.

In fact, the FBI's decision to deny employment to Weiler and Wright on the basis of their polygraph results is fully consistent with a more specific, relevant MIOG provision. Section 67-8.2.1(6)(b) states that for non-FBI personnel seeking FBI employment, applicants who "fail the initial polygraph examination yet deny practicing deception or withholding information will be disqualified from further processing except in those circumstances where an appeal has been granted." As Weiler and Wright's appeals were denied, they were accordingly disqualified from further consideration. Therefore, Plaintiffs' claims based on the FBI MIOG fail as a matter of law.

Conclusion

The Court finds that Plaintiffs' constitutional claims fail as a matter of law. Plaintiffs' APA claims are dismissed for lack of jurisdiction because they are precluded by the CSRA. In the alternative, Plaintiffs' APA claims based on Defendants' regulations are rejected as a matter of law, and any other APA claims are barred because they challenge actions committed to the agencies' discretion.

Accordingly, Plaintiffs' motion for summary judgment is **DENIED** and Defendants' motion to dismiss in part and for summary judgment is **GRANTED.** An appropriate Order accompanies this Memorandum Opinion.

Signed: Emmet G. Sullivan
United States District Judge
September 29, 2006

Endnotes

[i] The parties have admitted that all of the following facts are not in dispute.

[iiii] Though Plaintiffs have introduced significant evidence on the question of whether polygraph examinations are reliable, the Court need not answer that question to resolve Plaintiffs' claims. Therefore, the Court will not delve into the details of the polygraph examination process.

[iii] Plaintiffs cite to several cases, *White v. OPM,* 787 F.2d 660 (D.C. Cir. 1986), *Waltentas v. Lipper,* 636 F. Supp. 331 (S.D.N.Y. 1986), and *Doe v. United States Civil Service Commission,* 483 F. Supp. 539 (S.D.N.Y. 1980), to argue that job applicants have the same due process rights as employees. These cases are inapposite, however, because they discuss "stigma or disability"-type due process claims. *See White,* 787 F.2d at 665; *Waltentas,* 636 F. Supp. at 337; *Doe,* 483 F. Supp. at 569-70.

[iv] It is unclear whether a published statement must be false in order to constitute a "stigma or disability." The Court, however, will assume that dissemination of Plaintiffs' polygraph results does constitute a "stigma or disability" because the results call into question Plaintiffs' fitness for law enforcement positions.

[v] Plaintiffs attempt to establish that merely having damaging information in personnel files is sufficient to show that access to a profession has been foreclosed. Precedent from this Circuit, however, demonstrates what is lacking in this case. In *Old Dominion Dairy v. Secretary of Defense,* 631 F.2d 953 (D.C. Cir. 1980), the court recognized a valid due process claim because there was direct evidence that damaging information led to specific denials of government contracts for a private contractor. *Id.* at 955-59. Plaintiffs have presented no such evidence in this case.

[vi] *See* Defs.' Ex. 1 at 49-50 (deposition of Gregory Gilmartin); Defs.' Ex. 13 at 152-53 (deposition of Scott Myers).

[vii] Plaintiffs make much of the fact that the Secret Service asks applicants whether they have had sex with animals. The record shows, however, that the agency's question to applicants is whether they have ever committed a "serious crime," and the polygraph examiner explains what is meant by a "serious crime" by showing the applicant a list of crimes the agency considers to be serious. Sex with animals happens to be on that list, along with 28 other crimes. Defs.' Ex. 26 at 73-75 (deposition of Scott Myers); Defs.'Ex. 27 (list of crimes).

[viii] For support, Plaintiffs rely on one case from the Ninth Circuit, *Thorne v. El Segundo,* 726 F.2d 459 (9th Cir. 1983) (holding that inquiry into sexual history of a police officer applicant violated her constitutional right to privacy because the questioning was not narrowly tailored). *Thorne,* however, rested principally on the facts that there were absolutely no standards or guidelines for the detailed questioning of the applicant's sexual history, and that her admission of an affair with a police officer was one of the reasons she was denied employment. *See id.* at 469-71. Plaintiffs have made no such allegations in this case.

[ix] Plaintiffs contend that Defendants are estopped from arguing that the CSRA precludes their APA claims. They state that Defendants' rejection letters to the Plaintiffs did not discuss remedies available under the CSRA, and Plaintiffs were unaware of such remedies. Estoppel against the government, even if such claims are allowed, requires a showing of affirmative government misconduct. *See* Int'l *Union v. Clark,* 2006 WL 2598046, at *12 (D.D.C. 2006). In addition, the Supreme Court has found that the provision of erroneous information, without more, cannot give rise to an equitable estoppel claim against the Government. *See Office of Personnel Management v. Richmond,* 496 U.S. 414, 428-29 (1990). As Plaintiffs have made no showing of misconduct, and their argument concerns only the provision of information, Plaintiffs' estoppel argument is rejected.

[x] The Defendants' argument that the APA claims are also precluded by the Privacy Act, however, is unavailing. The Privacy Act, 5 U.S.C. § 552a, gives federal agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the government's part to comply with the requirements. *Maydak v. United States,* 363 F.3d 512, 515 (D.C. Cir. 2004). While the Privacy Act may address Plaintiffs' due process claims concerning the dissemination of their polygraph results, the Act does not address their APA claims, which attack Defendants' hiring decisions and processes. Therefore, the Privacy Act does not preclude APA review in this case. *See 5* U.S.C. § 701(a).

[xi] Excerpts of the MIOG were submitted as "Exhibit 32" to Plaintiffs' Motion for Summary Judgment.

Annual Review of Developments in Instructions 2005[1]

Colonel Michael J. Hargis[2], Lieutenant Colonel Timothy Grammel[3]

Abstract

This annual installment of developments in instructions covers cases decided by military appellate courts during the Court of Appeals for the Armed Forces' (CAAF) 2005 term.[i] As with earlier reviews on instructions, this article addresses new cases from the perspective of substantive criminal law, evidence, and sentencing. This article is written for military trial practitioners, and it frequently refers to the relevant paragraphs in the *Military Judges' Benchbook (Benchbook).*[ii] The *Benchbook* remains the primary resource for drafting instructions.

Substantive Criminal Law

Military Judge's Responsibility to Determine Lawfulness of an Order: United States v. Deisher[iii]

Obedience to lawful orders is at the very heart of military discipline. In *United States v. New,*[iv] the CAAF held that, in a case involving an order to wear United Nations accoutrements with the U.S. Army uniform, the military judge properly decided the issue of lawfulness of the order as a question of law. In *United States v. Jeffers,*[v] where the accused challenged the necessity of his company commander's no-contact order, the CAAF reiterated that lawfulness is a question of law. The court held that the military judge did not err in determining lawfulness of the alleged order and not submitting the issue to the members. Since *New,* it is black letter law that the legality of an order is a question of law to be decided by the military judge. When questions of fact and law are inextricably intertwined, however, the procedural steps for applying this rule may be confusing. In *United States v. Deisher,* the CAAF provided additional guidance to military judges on their responsibilities when the lawfulness of an order is at issue.

Airman (Amn) Deisher was charged, *inter alia,* with failure to obey a lawful order from Staff Sergeant (SSgt) Hazen, a Security Forces Investigator, to have no contact with Amn Pennington.[vi] During a pretrial session, the defense counsel moved to dismiss the charge because it did not have the legal attributes of a lawful order. The defense counsel argued that the communication lacked the clarity of a lawful order, did not have a definite duration, and exceeded the investigator's authority.[vii] The parties litigated the motion based on two exhibits—a memorandum from SSgt Hazen written a month after the incident and subsequent testimony at the Article 32 investigation.[viii] The trial counsel argued that the panel members, rather than the military judge, should resolve the issue of lawfulness of the order.[ix] The defense counsel disagreed. When the military judge suggested that the question of whether the order had been given was a question of fact to be decided by the members, the defense counsel responded that that was only one of the questions at issue, and the military judge had to resolve the remaining questions raised by the defense counsel.[x]

[1]The following article is reprinted from The Army Lawyer, Department of the Army Pamphlet 27-50-395: Lieutinant Colonel Christopher T. Fredrikson, "I Really Didn't Say Everything I Said: Recent Developments in Self-Incrimination Law", April 2006. The opinions and views expressed herein are those of the individual author, and do not necessarily represent the views of the Judge Advocate General's School, the United States Army, or any other governmental agency.

[2]Circuit Judge, 4th Judicial Circuit, United States Army Trial Judiciary, Fort Carson, Colorado

[3]Circuit Judge, 3d Judicial Circuit, United States Army Trial Judiciary, Fort Riley, Kansas

The military judge denied the motion to dismiss.[xi] The military judge's written ruling included the following:

Based on the proffered facts, the court cannot find as a matter of law the alleged order was unlawful. The defense motion is essentially an argument that the evidence is insufficient to establish either that an order was given or that it was lawful. These are questions of fact for the members to determine.[xii]

During the trial on the merits, SSgt Hazen testified that he was investigating the accused concerning an altercation with Amn Pennington. Staff Sergeant Hazen testified that he initially issued a no-contact order to the accused in a vehicle on the way to the medical clinic. Staff Sergeant Hazen could not recall the specific words, but he testified that when the accused expressed concern about what might happen to him, SSgt Hazen told the accused, "Let's get this behind you. Don't worry about it. Just don't have any more contact with Pennington. Don't get yourself in any more trouble."[xiii] Staff Sergeant Hazen testified that the accused responded with "I know. I know."[xiv]

Staff Sergeant Hazen testified that he issued a second no-contact order at the clinic in front of the accused's first sergeant. Staff Sergeant Hazen testified that, to the best of his recollection, he said to the accused, "In front of your first sergeant, I'm giving you a lawful order to have no contact with Airman Pennington; and if he approaches you, let somebody in your chain of command know or let me know and we'll take care of it as soon as possible."[xv] Staff Sergeant Hazen testified that the accused nodded his head.[xvi]

Staff Sergeant Hazen testified that he issued a third no-contact order on the way from the clinic to the base. He testified that he said, "You could make a career out of this. Let's not screw up any more, and don't have any more contact with Pennington."[xvii] Staff Sergeant Hazen testified that the accused acknowledged this statement with something to the effect of "I know. I know. I'm going to stay out of trouble. I'm going to be okay."[xviii]

During cross-examination, SSgt Hazen stated that the only statement he felt comfortable testifying under oath about was the statement at the clinic.[xix] Also, SSgt Hazen did not mention any no-contact orders in his report, and he did not speak to the accused's chain of command about the no-contact orders.[xx]

After instructing the members on the elements of violating a lawful order, the military judge instructed the members on what is required for an order to be lawful.[xxi] The military judge gave the instruction from the old note 4 to paragraph 3-16-2 of the *Benchbook.*[xxii] The CAAF issued its opinion in *United States v. New six* months before the trial in *Deisher,*[xxiii] but the model instruction in the *Benchbook* had not yet been changed.[xxiv]

The CAAF held that the military judge erred when he ruled that both the predicate factual aspects of the issue of lawfulness and the actual issue of lawfulness were matters to be resolved by the members.[xxv] The court reiterated that "the legality of the order is an issue of law that must be decided by the military judge, and not the court-martial panel."[xxvi] In the previously quoted language of the military judge's ruling, it was unclear whether the military judge made an affirmative determination that the order was lawful. The CAAF found a "significant likelihood" that the military judge did not do so and that the issue was resolved only by the panel.[xxvii] The court reversed the conviction of failure to obey a lawful order and set aside the sentence.[xxviii]

In ruling on a motion to dismiss on grounds that the alleged order was unlawful, the military judge should make a preliminary ruling whether certain communication under a set of specific circumstances constitutes a lawful order. This finding may necessarily require the military judge to make threshold contingent factual conclusions to determine whether the order at issue was lawful. This preliminary ruling on the lawfulness of an order, however, does not relieve the government of its burden to prove each element of the offense. The court-martial panel must still resolve all factual issues pertinent to the elements.[xxix]

Deisher confirms that the lawfulness of an order is a question of law that must be decided by the military judge. It also clarifies that a military judge need not instruct the members on what is required for an order to be lawful. The military judge must resolve any necessary preliminary factual questions relating to lawfulness and determine the lawfulness of the order.

Conspiracy to Commit Unpremeditated Murder

In *United States v. Shelton,*[xxx] the CAAF reversed a conviction for conspiracy to commit unpremeditated murder.[xxxi] *Shelton* highlights an important point concerning the mens rea requirement for the offense of conspiracy under Article 81 of the Uniform Code of Military Justice (UCMJ). If the underlying offense has an element requiring a certain result, then the agreement must include the intent to achieve that result.

It is important to remember that lawfulness of the order is not an element, so factual issues pertinent to lawfulness do not need to be submitted to the members, unless they are also pertinent to one or more of the elements. Sergeant (SGT) Shelton was charged with, inter alia, the premeditated murder of Private First Class (PFC) Chafin and conspiracy with SGT Seay to commit the premeditated murder of PFC Chafin.[xxxii] In accordance with the defense counsel's request, the military judge instructed the members of the court on the lesser included offenses of unpremeditated murder and conspiracy to commit unpremeditated murder.[xxxiii] When instructing on the elements of unpremeditated murder, the military judge properly instructed the members that the offense required that "at the time of the killing, the accused had the intent to kill or inflict great bodily harm on PFC Chafin."[xxxiv] When instructing on the elements of conspiracy to commit unpremeditated murder, the military judge properly instructed the members that the offense required that the accused "entered into an agreement with SGT Bobby D. Seay II to commit unpremeditated murder."[xxxv] However, when providing the required instruction on the elements of the offense within which the accused was charged—conspiracy to commit premeditated murder—the military judge instructed the members that the elements of the object of the conspiracy were "the same as set forth in the instruction on the lesser included offense of unpremeditated murder," without specifically repeating the elements.[xxxvi] The officer panel convicted the accused of, inter alia, unpremeditated murder and conspiracy to commit unpremeditated murder.[xxxvii]

Based on these instructions, the CAAF found that the members could have convicted the accused of conspiracy to commit unpremeditated murder based on an intent to inflict great bodily harm.[xxxviii] The court held that, "[i]f the intent of the parties to the agreement was limited to the infliction of great bodily harm, their agreement was to commit aggravated assault, not unpremeditated murder."[xxxix] Therefore, the CAAF affirmed a finding of guilty of only the lesser included offense of conspiracy to commit aggravated assault.[xl]

Although the court did not discuss at any length the law of conspiracy, a brief analysis of the elements of the offense will show the court was correct. The two elements of a conspiracy are: (1) an agreement to commit an offense under the Uniform Code of Military Justice; and (2) an overt act by one or more of the conspirators to effect the object of the conspiracy.[xli] The issue in this case involved the first element. The agreement must be to bring about the actual commission of the offense. If one of the elements of the offense requires a certain result, such as the death of a person, then a conspiracy to commit that offense would require an agreement to bring about that result.[xlii] Therefore, even though an intent to either kill or inflict great bodily harm is sufficient for unpremeditated murder, conspiracy to commit unpremeditated murder would necessarily require an intent to kill.[xliii]

The trial practitioner can glean two lessons from this case. First, if an offense requires a certain result, then a conspiracy to commit that offense requires an agreement to bring about that result. This would apply not only to conspiracy to commit unpremeditated murder, but also to conspiracy to commit other offenses such as maiming. Second, military judges must be cautious when cross-

referencing during instructions on findings. It is unclear whether the military judge in this case intended to instruct the members that an intent to inflict great bodily harm was sufficient for conspiracy to commit unpremeditated murder or whether that was done inadvertently when cross-referencing to the instruction on unpremeditated murder that had already been given. In most cases where conspiracy and the underlying offense are charged, the military judge should first instruct on the underlying offense and then refer back to the elements and definitions when instructing on conspiracy. In cases like *Shelton,* however, the military judge should restate the elements of the underlying offense and highlight the differences for the members.

Variance by Excepting the Language "On Divers Occasions"

In *United States v. Augspurger,*[xliv] the CAAF again addressed an ambiguous finding of guilty resulting from the members excepting the words "on divers occasions" from a specification and not clearly disclosing upon which single occasion the conviction was based.[xlv]

Airman Basic Augspurger was charged, *inter alia,* with wrongfully using marijuana "on divers occasions" between 15 October 2001 and 20 February 2002.[xlvi] The government presented evidence of three separate allegations of wrongful use of marijuana. The evidence for one of the allegations consisted of a positive urinalysis result and a confession to smoking marijuana at an off-base apartment with friends on 1 December 2001. The evidence for the other two allegations consisted of the testimony of another Airman, who had been previously convicted of drug use, that he had seen the accused smoke marijuana on two separate occasions in January and February 2002. [xlvii]

The members found the accused guilty of the specification of wrongful use of marijuana except the words "on divers occasions."[xlviii] The members did not indicate on which of the three occasions they based their finding.[xlix] The defense counsel requested that the military judge have the members clarify their findings, but the military judge declined to do so.[l]

On appeal, the Air Force Court of Criminal Appeals (AFCCA) held that the military judge erred by not requiring the members to specify on which of the occasions they based their finding.[li] However, the AFCCA concluded that it was able to determine beyond a reasonable doubt that the members convicted the accused of the December 2001 use, and the Air Force court modified the findings to resolve the ambiguity.[lii]

The CAAF found that the Air Force court erred.[liii] When the accused is found guilty, except the words "on divers occasions," then the accused has been found *guilty* of misconduct on a single occasion and *not guilty* of the remaining occasions.[liv] "Where the findings do not disclose the single occasion on which the conviction is based, the Court of Criminal Appeals cannot conduct a factual sufficiency review or affirm the findings because it cannot determine which occasion the servicemember was convicted of and which occasion the servicemember was acquitted of."[lv]

In *Augspurger,* the CAAF makes it clear that it is the trial judge's responsiblity to ensure that the findings, as announced, clearly state the factual basis for the offense. During the trial, there are two opportunities for the military judge to accomplish this. First, during the instructions on findings, the military judge should instruct the members that if they except the words "divers occasions," they must specify which allegation was the basis of their finding. Second, if there is an ambiguity when the military judge is examining the findings worksheet prior to announcement, the military judge should instruct the members to clarify their findings.[lvi]

This case reiterates for trial practitioners the lessons learned from *Walters.* Fortunately, when this situation arises now, there are approved interim changes to the *Benchbook* that provide guidance and model instructions.[lvii] If a specification alleges "on divers occasions" and the evidence is such that the members might find the accused guilty of not more than one occasion, then the military judge should

provide an appropriate variance instruction. Also, the findings worksheet should be tailored to assist the members in announcing an unambiguous verdict. In addition, when reviewing the findings worksheet before the findings are announced, the military judge must instruct the members to clarify their findings if the worksheet shows a finding of guilty except the words "on divers occasions" without exceptions or substitutions specifying upon which occasion the finding of guilt is based. Because this situation is relatively common, trial practitioners must remain vigilant to avoid committing *a "Walters* violation."

Mental Responsibility and the Standard of Proof

In *United States v. Green,*[lviii] the AFCCA set aside a conviction for desertion.[lix] The central issue at trial was mental responsibility. The accused was a noncommissioned officer with nineteen years and six months on active duty. He absented himself from his unit and was living on the streets for several months.[lx] The defense provided evidence, including expert testimony, supporting its argument that the accused was not mentally responsible at the time of the offense.[lxi] The government's expert witness opined that the accused was not suffering from a mental disease or defect and was probably malingering.[lxii] The military judge gave the standard instruction on mental responsibility, including the definition of clear and convincing evidence as "proof which will produce . . . a firm belief or conviction as to the facts sought to be established."[lxiii] The military judge then gave the Air Force's tailored definition of proof beyond a reasonable doubt as "proof that leaves you firmly convinced of the accused's guilt."[lxiv]

The Air Force court concluded that the military judge erred in not adequately instructing the members on the distinction between these burdens of proof. During prefatory instructions to the members, the military judge instructed them that proof beyond a reasonable doubt is a more stringent standard than the preponderance standard generally used in administrative hearings.[lxv] However, the members were not instructed on any distinction between proof beyond a reasonable doubt and clear and convincing evidence.[lxvi] Because of the semantic similarity between "firm belief or conviction" and "firmly convinced," the court found that it was critical for the military judge to instruct the members on how to differentiate between the two standards.[lxvii] The Air Force court held, "When the 'clear and convincing' standard is employed, the military judge must, at a minimum, clearly instruct the members that it is an intermediate standard; higher than a mere probability, but not as high as 'proof beyond a reasonable doubt.'"[lxviii]

This case is significant for those practicing in the Air Force, but less important for those practicing in the other services. The potential confusion in this case was created by the language of the tailored Air Force instruction on "reasonable doubt" when it was used in conjunction with the standard Benchbook instruction on "clear and convincing evidence," along with distinguishing "proof beyond a reasonable doubt" from "preponderance of the evidence" but not "clear and convincing evidence." This potential confusion is not present when using the standard Benchbook instruction on "reasonable doubt" and when "proof beyond a reasonable doubt" is not distinguished from "preponderance of the evidence." However, a broader lesson for all from this case is that trial practitioners must strive to keep instructions clear and understandable for the court members.

Evidence

Character for Truthfulness: United States v. Diaz[lxix]

Chief Petty Officer Diaz testified on his own behalf at trial and several witnesses testified to his character for truthfulness. Prior to instructions, the defense requested Instruction 7-8-1 from the Benchbook regarding the accused's character for truthfulness. Specifically, the defense sought the language that states "[e]vidence of the accused's character for truthfulness may be sufficient to cause a reasonable doubt as to his guilt."[lxx] The military judge denied the

defense request, stating that truthfulness was not a pertinent character trait given that the accused was charged with molesting his daughter.[lxxi]

The NMCCA agreed with the military judge that truthfulness was not a pertinent character trait in this case under Military Rule of Evidence (MRE) 404(a)(1). Accordingly, the accused's character for truthfulness did not "bear directly on guilt or innocence,"[lxxii] and the requested instruction was not legally correct. Recognizing that the testimony was offered only to support the accused's character for truthfulness after it had been attacked at trial (under M.R.E. 608(a)), the NMCCA held the military judge correctly instructed the members that they could consider the proffered character evidence when determining the accused's believability.[lxxiii]

This case illustrates the different ways that evidence of an accused's character for truthfulness may apply in any given case. When charged with an offense for which a truthful character trait would be "pertinent," such as false official statement, Instruction 7-8-1 may be appropriate.[lxxiv] However, if truthfulness is not a "pertinent" character trait, evidence of such a character trait is admissible only as it bears on the accused's credibility,[lxxv] and Instruction 7-8-3 of the Benchbook should be used.

Article 112a and the Inference of Wrongfulness: United States v. Brewer[lxxvi]

Air Force Master Sergeant (MSgt) Ronald Brewer was charged with wrongful use of marijuana. The government's evidence consisted of both urinalysis and hair analysis test results. At trial, the government relied upon the permissible inference to show the accused's use of marijuana was wrongful.[lxxvii]

At trial, the military judge strayed from the model Article 112a instructions in the *Benchbook*, instructing the officer and enlisted members as follows:

> To be punishable under Article 112a, use of a controlled substance must be wrongful. Use of a controlled substance is wrongful if it is without legal justification or authorization.
>
> Use of a controlled substance is not wrongful if such act or acts are: (a) done pursuant to legitimate law enforcement activities (for example, an informant who is forced to use drugs as part of an undercover operation to keep from being discovered is not guilty of wrongful use); (b) done by authorized personnel in the performance of medical duties or experiments; or (c) done without knowledge of the contraband nature of the substance (for example, a person who uses marijuana, but actually believes it to be a lawful cigarette or cigar, is not guilty of wrongful use of marijuana).
>
> Use of a controlled substance may be inferred to be wrongful in the absence of evidence to the contrary. However, the drawing of this inference is not required.
>
> *The burden of going forward with evidence with respect to any such exception in any court-martial shall be upon the person claiming its benefit.*
>
> *If such an issue is raised by the evidence presented, then the burden is on the United States to establish that the use was wrongful.*
>
> Knowledge by the accused of the presence of the substance and knowledge of its contraband nature may be inferred from the surrounding circumstances. However, the drawing of the inference is not required.
>
> [T]he burden of proof to establish the guilt of the accused beyond a reasonable doubt is on the government. The burden never shifts to the accused to establish innocence or to disprove the facts necessary to establish each element of the offense.[lxxviii]

On appeal, MSgt Brewer challenged the military judge's instructions as erroneous. The CAAF found the military judge's instructions had turned the permissive inference of wrongfulness into an

improper "mandatory rebuttable presumption" and reversed.[lxxix]

The CAAF focused on the two paragraphs above in italics—taken from the explanation section of the *Manual for Courts-Martial* and not found in the model instruction contained in the *Benchbook.* The CAAF held that the military judge's failure to explain the term "burden of going forward" and use of the term "exception" may have led the members to believe the accused had a "responsibility to prove that one of the exceptions applies" or that only when the accused so proves does the burden "shift[] back to the Government to show wrongful use."[lxxx] As a result, the CAAF found a reasonable member could have interpreted the instructions as saying wrongfulness was presumed unless the accused proved an exception, thus improperly creating a mandatory presumption of wrongfulness.[lxxxi]

The CAAF found error in the portions of the instruction taken from the *MCM* (and not included in the model *Benchbook* instruction). Importantly, *Brewer* does not hold that the Article 112a *Benchbook* instruction regarding the permissive inference of wrongfulness is erroneous.[lxxxii] Had the military judge used the *Benchbook* instruction, instructional error likely would not have occurred.

Findings Arguments Run Amuck: Comment on Constitutional Rights

United States v. Carter[lxxxiii]

Airman Carter was charged with committing indecent acts with Amn D while he and Amn D were alone in a barracks room. Airman D was the only government witness and the defense presented no evidence, instead focusing only on challenging the alleged victim's credibility.[lxxxiv]

During opening argument on findings, the trial counsel repeatedly referred to the government's evidence of the accused's misconduct as "uncontroverted" or "uncontested."[lxxxv] At the conclusion of the defense argument on findings, the military judge instructed the members that the accused had an absolute right not to testify and the members must disregard the accused's failure to testify.[lxxxvi] Significantly, after defense argument, the trial counsel in rebuttal again repeated the theme that the government evidence was "uncontradicted."[lxxxvii] The military judge did not further instruct the members on the accused's right to remain silent and the panel later returned a finding of guilty. The AFCCA reversed, finding plain error.[lxxxviii] The Air Force Judge Advocate General certified the issue for review by the CAAF.[lxxxix]

Reviewing the totality of the situation, the CAAF affirmed the AFCCA's reversal, finding the trial counsel's comments to be impermissible comments on the accused's right to remain silent, which shifted the burden of proof from the government.[xc]

Although the Discussion to Rule for Court-Martial (RCM) 919(b)[xci] does not explicitly preclude trial counsel from arguing the government's evidence is unrebutted, when the accused and the victim are the only two people present at the time of the alleged offenses, certainly the direct implication is that the rebuttal must come from the accused.[xcii] Thus, such comments by the government are improper.

Defense counsel must be alert to situations that could be interpreted as a comment on their client's right to remain silent and must object.[xciii] Likewise, even without defense objection, the military judge should sua sponte instruct the members on the accused's right to remain silent, the presumption of innocence, and the burden of proof[xciv] when the trial counsel's argument implies the defense has an obligation to present evidence.[xcv]

Findings Arguments Run Amuck: A Litany

United States v. Fletcher[xcvi]

Technical Sergeant Fletcher elected to be tried by members and took the stand in his own defense. He denied using cocaine and presented evidence of his character for truthfulness, his church affiliation, and his good family life.[xcvii]

Tempers apparently flared between

trial and defense counsel during trial. During the findings argument, the trial counsel inappropriately injected her own personal beliefs and opinions, improperly vouched for the government's evidence and witnesses, provided her own personal views of the evidence and the accused's guilt, and made disparaging remarks about both the defense counsel and the accused's credibility.[xcviii]

There were no defense objections to the majority of the trial counsel's improper actions. Finding plain error, however, the CAAF reversed.[xcix]

Addressing the role of the military judge during argument, the CAAF again reiterated that curative instructions by the military judge (even absent objection) may remedy an error. The CAAF noted that the military judge "did not make any effort to remedy any misconduct other than a few statements to which defense counsel objected."[c] Although the military judge provided the standard *Benchbook* instruction that the arguments of counsel are not evidence,[ci] he took no further action in response to the trial counsel's argument.

As a repeated theme this term, the CAAF touched upon the military judge's sua sponte obligation to give corrective instructions to the members in response to improper argument by counsel. Whether the improper argument is by the government or the defense, the military judge should be prepared to interrupt, advise the members that the objectionable portion of the argument is improper and direct them to disregard it.[cii]

The Military Judge Going Too Far: Instructing on the Accused's Failure to Testify:

United States v. Forbes[1ciii]

At his court-martial, Quartermaster First Class Forbes did not testify. Concerned that the members might draw an adverse inference from his silence, the military judge told counsel that he intended to give the standard *Benchbook* instruction on the accused's failure to testify.[civ] The defense objected. The military judge decided to give the instruction anyway.[cv]

Last year's annual review of instructions article discussed the NMCCA response to this case. On appeal, the NMCCA held that giving the instruction over defense objection was error and, applying a presumption of prejudice, found the error prejudicial.[cvi]

When evaluating whether the military judge properly gave the instruction over defense objection, the NMCCA said the military judge must balance the defense objection to the request against the "case-specific interests of justice."[cvii] By analogy, the NMCCA compared that balancing to the balancing test under MRE 403. The NMCCA stated the deference they would give the military judge's analysis as follows:

> When a military judge gives a fail-to-testify instruction over defense objection after having identified the case-specific "interests of justice" that support his decision and articulating his analysis of those interests relative to the defense election, then he should be accorded great deference under a standard of review of abuse of discretion. If he identifies the interests of justice in question but does not articulate his balancing of those interests with the defense election, he is accorded less deference. If he does not identify interests of justice at all, the standard of review is de novo.[cviii]

If the reviewing court finds error on the military judge's part, the NMCCA said prejudice to the accused should be presumed, with the government bearing the burden to rebut it:

> When a military judge commits error by giving this instruction over defense objection in the absence of articulated case-specific interests of justice, a presumption of prejudice results. The Government then bears the burden of showing by a preponderance of the evidence why the appellant was not prejudiced by the instruction. Admittedly, this may be a difficult burden for the

> Government to bear. But, this court did not write the Rule, and on the issue of an appropriate test for prejudice, we feel compelled to take our cues from the President's language that so clearly favors the military accused.[cix]

Finding the military judge had erred and that the government had not carried its burden, the NMCCA reversed.

The Judge Advocate General of the Navy certified two questions to the CAAF: (1) Did the NMCCA err in finding the instruction was error, and (2) Did the NMCCA err in presuming prejudice?[cx] The CAAF answered no to both questions, specifically adopting the NMCCA's framework for review.[cxi]

Citing MRE 301(g),[cxii] the CAAF emphasized that the decision to give this instruction belongs to the defense, with one exception. The military judge may give the instruction over defense objection when it is "necessary in the interests of justice."[cxiii]

The reason given by the military judge was to "protect the accused from any adverse feelings by the members."[cxiv] The CAAF determined that this "generalized fear" alone is insufficient to override the defense decision against the instruction.[cxv] Unfortunately, the military judge made no "case-specific" findings of necessity, nor did he articulate his analysis of those against the defense objection to the instruction. Finding no case-specific circumstances in their de novo review, the CAAF affirmed the NMCCA's reversal.[cxvi]

In future cases, if the military judge gives the failure to testify instruction over defense objection, the trial counsel should ensure that the military judge makes "case specific" findings of necessity on the record and articulates why those factors outweigh the defense objection to the instruction.[cxvii]

The Military Judge Going Too Far: Comment on Right to Silence:

United States v. Andreozzi[cxviii]

During Staff Sergeant (SSG) Andreozzi's general court-martial for a litany of serious offenses against his wife, the defense called a high school friend as a character witness. Three times during that witness's testimony, he stated the accused had told him he wanted to "preserve his marriage."[cxix] The military judge sustained the first objection. The military judge also sustained the second objection, but in addition told the members "to disregard the 'testimony with regard to what [the accused] might have told his friend.'"[cxx] In apparent frustration, the military judge gave the following instruction after sustaining the third objection:

> Members of the court, you can't consider that part of the testimony. It[']s not before you. It is hearsay testimony. The trial counsel has not had an opportunity to cross examine the person who allegedly made the statement; therefore you may not consider it.[cxxi]

The military judge denied a motion for mistrial based upon improper comment on the accused's right to silence.[cxxii] When the defense rested without the accused testifying, the military judge gave the standard *Benchbook* instruction on the accused's right to silence. He gave the instruction again during findings instructions.

On appeal, the Army Court of Criminal Appeals (ACCA) determined that the military judge's third instruction to the members was an erroneous comment on the accused's right to silence.[cxxiii] Given the two specific instructions on the accused's right to silence, however, the ACCA determined the error was harmless and affirmed.

Trial work can be a frustrating business for military judges and counsel. Attempts by military judges to educate the members as to why certain evidence is impermissible, borne of that frustration, may also inadvertently result in constitutional error. Ruling upon the objection, without comment further than assuring the members will disregard the evidence, may be advisable in such challenging situations.

Sentencing

Unsworn Statements and Sentence Comparison: United States v. Barrier[cxxiv]

Following his conviction for wrongfully using drugs, Senior Airman (SrAmn) Barrier included the following in his unsworn statement to the members:

When deciding whether your sentence should include some amount of confinement, I know that each case has to be decided on its own merits. But I also believe that similar cases should receive similar punishments. Such as last year, Senior Airman Watson from Tyndall was charged with using ecstasy and the confinement portion of his sentence was only three months.[cxxv]

Senior Airman Watson was not a co-accused nor was he charged with conspiring with Barrier—he was merely another airman convicted of drug use. After the accused's unsworn statement, the military judge, over defense objection, gave the following instruction to the members, based on the 2000 AFCCA case of *United States v. Friedmann*:[cxxvi]

> Now, during the accused's unsworn statement, he alluded to a case of another individual who the accused had stated had received a certain degree of punishment. In rebuttal, the trial counsel offered you Prosecution Exhibit 6, which was the court-martial order from that case which stated what that individual got in that case.
>
> The reason I mention this is for the following reason, and that is because, in fact, the disposition of other cases is irrelevant for your consideration in adjudging an appropriate sentence for this accused. You did not know all the facts of those other cases, or other cases in which sentences were handed down, nor anything about those accused in those cases, and it is not your function to consider those matters at this trial. Likewise, it is not your position to second guess the disposition of other cases, or even try to place the accused's case in its proper place on the spectrum of some hypothetical scale of justice.
>
> Even if you knew all the facts about other offenses and offenders, that would not enable you to determine whether the accused should be punished more harshly or more leniently because the facts are different and because the disposition authority in those other cases cannot be presumed to have any greater skill than you in determining an appropriate punishment.
>
> If there is to be meaningful comparison of the accused's case to those of other [sic] similarly situated, it would come by consideration of the convening authority at the time that he acts on the adjudged sentence in this case. The convening authority can ameliorate a harsh sentence to bring it in line with appropriate sentences in other similar cases, but he cannot increase a light sentence to bring it in line with similar cases. In any event, such action is within the sole discretion of the convening authority.
>
> You, of course, should not rely on this in determining what is an appropriate punishment for this accused for the offenses of which he stands convicted. If the sentence that you impose in this case is appropriate for the accused and his offenses, it is none of your concern as to whether any other accused was appropriately punished for his offenses.
>
> You have the independent responsibility to determine an appropriate

sentence, and you may not adjudge an excessive sentence in reliance upon mitigation action by higher authority.[cxxvii]

On appeal, SrA Barrier argued the military judge interfered with his "largely unfettered" right to provide information in his unsworn statement.[cxxviii] The CAAF disagreed and affirmed. Providing further guidance to the bench and bar, the CAAF stated that when the accused brings such sentence comparison information to the attention of the members, the military judge may appropriately address three areas.[cxxix] First, the military judge may tell the members "that in the military justice system[,]. . . the members are required to adjudge a sentence based upon their evaluation of the evidence without regard to the disposition of other cases. . . ."[cxxx] Second, the military judge's instruction may say "to the extent that the [military justice] system provides for sentence comparison, that function is not part of the members' deliberations; [but] it is a power assigned to the convening authority and Court of Criminal Appeals. . . ."[cxxxi] Finally, the military judge may tell the members "in the course of determining an appropriate punishment, . . . [they] may not rely upon the possibility of sentence reduction by the convening authority or the Court of Criminal Appeals."[cxxxii]

Significantly, the court said that such sentence comparison evidence—not of a co-accused, but merely of someone similarly situated—is irrelevant as extenuation and mitigation under RCM 1001 and may be appropriately excluded "if the military judge determines that an instruction would not suffice to place the statement in proper context for the members."[cxxxiii]

This language is a narrowing of the court's opinion in *United States v. Grill,* where the military judge was reversed for barring the accused from referring in his unsworn statement to the sentences received by his civilian co-accused.[cxxxiv]

Unsworn Statements and Polygraph Evidence:

United States v. Johnson[cxxxv]

Although not specifically involving an instructions issue, this case is another in the CAAF's trend this term to restrict the information presented to the court by an accused through an unsworn statement.

Technical Sergeant Johnson was accused of trafficking in marijuana. Before trial, he took a private polygraph test after which the examiner concluded the accused was not deceptive. Notwithstanding, the accused was tried and convicted. Prior to making his unsworn statement at trial, the accused apparently provided the substance of that statement to the military judge. His proposed unsworn statement referred to passing the polygraph test. The military judge prohibited him from including any reference to his exculpatory polygraph test in his unsworn statement.[cxxxvi]

Citing *Grill* for the proposition that the allocution right in an unsworn statement is largely unfettered and broadly construed, the accused argued that the military judge erred in preventing him from addressing the polygraph in his unsworn statement. On appeal, the CAAF disagreed and affirmed.[cxxxvii]

Discussing the unsworn statement and its limits, the court said the unsworn statement "remains a product of RCM 1001(c) and thus remains defined in scope by the rule's reference to matters presented in extenuation, mitigation and rebuttal."[cxxxviii] Finding that an exculpatory polygraph result does not fit into any of these categories, but instead is contrary to existing caselaw that prohibits relitigating findings during sentencing,[cxxxix] the CAAF found the military judge appropriately excluded those references from the accused's unsworn statement.

Although *Grill* allows the military judge to appropriately instruct the members on how to use otherwise inadmissible information from an unsworn statement, *Barrier* makes clear that the military judge may use his discretion to prohibit some information outright, instead of later instructing the members. *Johnson* goes one step further and makes clear that information conveyed through the unsworn

statements must meet the definitional requirements of RCM 1001(c) as either extenuation, mitigation, or rebuttal, before it is a permissible part of an unsworn statement.

Unsworn Statements and a Co-Accused's Acquittal:

United States v. Sowell[cxl]

Seaman Stacie Sowell's situation rounds out the CAAF's handling of unsworn statements.

Seaman Sowell was charged with conspiracy and larceny involving government computers. Two co-conspirators were never charged, and a third, Petty Officer (PO) Elliot, was acquitted of "substantively identical charges."[cxli] Petty Officer Elliot testified for the accused that they never talked about stealing computers and never took any of the computers. Trial counsel challenged PO Elliot's credibility, arguing on findings that, as a co-conspirator, she had a motive to lie.[cxlii]

After her conviction, Seaman Sowell sought to tell the members that PO Elliott had been acquitted. The military judge prevented the accused from doing so.[cxliii]

On appeal, the accused contended that the military judge's actions interfered with her right to make an unsworn statement, as set forth in *Grill.* In response, government appellate counsel argued that reference to the acquittal would impeach the findings, as both the accused and Elliott faced the same charges. Additionally, the government argued that it would be impermissible sentence comparison, citing Mamaluy.[cxliv]

The CAAF agreed with the defense and reversed, but on different grounds.[cxlv] The CAAF held that under the specific facts of this case, trial counsel's argument on findings opened the door and therefore such a comment by the accused was proper rebuttal under RCM 1001(c). Because the trial counsel had referred to Petty Officer Elliott as a "co-conspirator," he implied that she was also guilty of the offenses with which the accused was charged. Thus, in the CAAF's view, what would otherwise have been improper extenuation and mitigation evidence became appropriate RCM 1001(c) rebuttal evidence, as part of an unsworn statement.[cxlvi]

The result notwithstanding, *Sowell* represents a continuation of the trend this term to limit the scope of the court's prior opinion in *Grill,* allowing the military judge more flexibility to deal with sentence comparison information in unsworn statements.

Conclusion

The cases from the CAAF's 2005 term provide many lessons on instructions for military justice practitioners. The *Benchbook* is the primary resource for instructions, and varying from the standard *Benchbook* instructions should only be done for good reason and with careful deliberation. The *Benchbook* should only be the first step, however, because it might not adequately reflect new caselaw or cover the law in a unique situation. Military judges must pay attention to detail in order to provide clear and accurate instructions to the members. Also, military judges must be ready to stop improper arguments and provide curative instructions. Instructions to the members require careful thought because they are critical to a fair trial.

Endnotes

[i][ii] The 2005 term began on 1 October 2004 and ended on 30 September 2005.

[ii] U.S. DEP'T OF ARMY, PAM. 27-9, LEGAL SERVICES: MILITARY JUDGES' BENCHBOOK (15 Sept. 2002) [hereinafter BENCHBOOK].

[iii] 61 M.J. 313 (2005).

[iv] 55 M.J. 95 (2001).

[v] 57 M.J. 13 (2002).

[vi] Deisher, 61 M.J. at 314.

[vii] *Id.*

[viii] *Id.*

[ix] *Id.* at 315.

[x] *Id.*

[xi] *Id.*

[xii] *Id.*

[xiii] *Id.*

[xiv] *Id.*

[xv] *Id.* at 315-16.

[xvi] *Id.* at 316.

[xvii] *Id.*

[xviii] *Id.*

[xix] *Id.*

[xx] *Id.*

[xxi] *Id.* at 317.

[xxii] See BENCHBOOK, supra note 2, para. 3-16-2 n.4.

[xxiii] Deisher, 61 M.J. at 318.

[xxiv] On 10 February 2004, the model instructions in paragraphs 3-14-2, 3-15-2, 3-16-1, 3-16-2, and 3-16-3 were changed to reflect the holding in United States v. New. Because of the CAAF's opinion in United States v. Deisher, the new note 4 in paragraph 3-16-2 and identical notes in paragraphs 3-14-2, 3-3-15-2, 3-16-1, and 3-16-3 do not accurately state the law. Those notes provide an instruction for those rare circumstances where the question of lawfulness is intertwined with questions of fact and should be submitted to the members with appropriate guidance. The issue of lawfulness does not ever need to be submitted to the members. However, the last two sentences of that note may be helpful as a format for an instruction, if the content of the order is in dispute and the military judge makes a preliminary ruling that an order with

specific language would be lawful but an order with other specific language would not be lawful. See BENCHBOOK, supra note 2, para. 3-16-2 (IC, 10 Feb. 2004).

[xxv] Deisher, 61 M.J. at 318.

[xxvi] *Id.* at 317.

[xxvii] *Id.* at 318.

[xxviii] *Id.* at 319.

[xxix] *Id.* at 317. It is important to remember that lawfulness of the order is not an element, so factual issues pertinent to lawfulness do not need to be submitted to the members, unless they are also pertinent to one or more of the elements.

[xxx] 62 M.J. 1 (2005).

[xxxi] *Id.* at 5. The court affirmed the lesser included offense of conspiracy to commit aggravated assault, the findings as to the remaining offenses, and the sentence. *Id.* The court consisting of officer members adjudged a sentence of a dishonorable discharge, confinement for life, total forfeiture of pay and allowances, and reduction to the grade of E-1. *Id.* at 2.

[xxxii] *Id.*

[xxxiii] *Id.*

[xxxiv] *Id.* at 4.

[xxxv] *Id.*

[xxxvi] *Id.*

[xxxvii] *Id.*

[xxxviii] *Id.* at 5.

[xxxix] *Id.*

[xl] *Id.*

[xli] UCMJ art. 81 (2005); see also MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, ¶ 5b (2005) [hereinafter MCM]; BENCHBOOK, supra note 2, para. 3-5-1c.

[xlii] See 2 WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 12.2(c)(2), at 276-79 (2d ed. 2003).

[xliii] Shelton, 62 M.J. at 5. Similarly, even though an intent to either kill or inflict great bodily harm is sufficient for unpremeditated murder, attempted unpremeditated murder requires a specific intent to kill. United States v. Roa, 12 M.J. 210, 212 (C.M.A. 1982); see BENCHBOOK, supra note 2, para. 3-4-2c.

[xliv] 61 M.J. 189 (2005).

[xlv] The CAAF has started to refer to this as a "Walters violation." See United States v. Scheurer, 62 M.J. 100, 112 (2005) (referring to United States v. Walters, 58 M.J. 391 (2003)).

[xlvi] Augspurger, 61 M.J. at 189-90.

[xlvii] *Id.* at 190.

[xlviii] *Id.*

[xlix] *Id.*

[l] *Id.*

[li] *Id.* at 191.

[lii] *Id.*

[liii] *Id.* at 192.

[liv] *Id.* at 190.

[lv] *Id.*

[lvi] *Id.* at 192.

[lvii] On 16 September 2003, after the Walters opinion, the Army Trial Judiciary approved an interim change (IC) to the Benchbook that added the new paragraph 7-25. It contains notes with guidance for the military judge, the definition for "divers occasions," and a model instruction for the members when the military judge's review of the findings worksheet reveals a finding of guilty except the words "on divers occasions" without specifying which one occasion. See BENCHBOOK, supra note 2, para. 7-25 (IC, 16 Sept. 2003).

[lviii] 62 M.J. 501 (A.F. Ct. Crim. App. 2005).

[lix] *Id.* at 504.

[lx] *Id.* at 502.

[lxi] *Id.*

[lxii] *Id.* at 502-03.

[lxiii] *Id.Id.* at 503. The Benchbook provides the following definition for "clear and convincing evidence. By clear and convincing evidence I mean that measure or degree of proof which will produce in your mind a firm belief or conviction as to the facts sought to be established. The requirements of clear and convincing evidence does not call for unanswerable or conclusive evidence. Whether the evidence is clear and convincing requires weighing, comparing, testing, and judging its worth when considered in connection with all the facts and circumstances in evidence. BENCHBOOK, supra note 2, para. 6-4.

[lxiv] Green, 62 M.J. at 503.

[lxv] *Id.* Although the opinion does not quote this part of the instructions given to the members in this case, the Air Force Supplement to the Benchbook contains the following definition of "reasonable doubt" in both the Preliminary Instructions in paragraph 2-5 and the Closing Substantive Instructions on Findings in paragraph 2-5-12.
A "reasonable doubt" is a conscientious doubt, based upon reason and common sense, and arising from the state of the evidence. Some of you may have served as jurors in civil cases, or as members of an administrative board, where you were told that it is only necessary to prove that a fact is more likely true than not true. In criminal cases, the government's proof must be more powerful than that. It must be beyond a reasonable doubt. Proof beyond a reasonable doubt is proof that leaves you firmly convinced of the accused's guilt. There are very few things in this world that we know with absolute certainty, and in criminal cases the law does not require proof that overcomes every possible doubt. If, based on your consideration of the evidence, you are firmly convinced that the accused is guilty of the offense charged, you must find (him) (her) guilty. If, on the other hand, you think there is a real possibility that the accused is not guilty, you must give (him) (her) the benefit of the doubt and find (him) (her) not guilty.

U.S. DEP'T OF ARMY, PAM. 27-9, LEGAL SERVICES: MILITARY JUDGES' BENCHBOOK para. 2-5 (15 Sept. 2002) (Air Force Supplement).
The standard *Benchbook* preliminary instruction on "reasonable doubt" is a follows.

> A reasonable doubt is an honest, conscientious doubt, suggested by the material evidence, or lack of it, in the case. It is an honest misgiving generated by insufficiency of proof of guilt. Proof beyond a reasonable doubt means proof to an evidentiary certainty, although not necessarily to an absolute or mathematical certainty. The proof must exclude every fair and reasonable hypothesis of the evidence except that of guilt.
> BENCHBOOK, *supra* note 2, para. 2-5. The standard Benchbook closing substantive instruction on "reasonable doubt," when mental responsibility is in issue, is a follows.
> By reasonable doubt is intended not a fanciful or ingenious doubt or conjecture, but an honest, conscientious doubt suggested by the material evidence or lack of it in the case. It is an honest misgiving generated by insufficiency of proof of guilt. Proof beyond a reasonable doubt means proof to an evidentiary certainty although not necessarily to an absolute or mathematical certainty. The proof must be such as to exclude not every hypothesis or possibility of innocence, but every fair and rational hypothesis except that of guilt.
> *Id.* para. 2-5-12. This instruction is virtually identical to the closing substantive instruction when mental responsibility is not in issue, except for some quotation marks and a comma that are insubstantial.

[lxvi] Green, 62 M.J. at 503.

[lxvii] *Id.*

[lxviii] *Id.* at 504. The court further suggested, when the need for an instruction on "clear and convincing evidence" is apparent at the beginning of trial, providing a tailored instruction distinguishing between the various burdens of proof instead of the standard Air Force instruction discussing only preponderance and beyond a reasonable doubt. *Id.* n.4.

[lxix] 61 M.J. 594 (N-M. Ct. Crim. App. 2005).

[lxx] See BENCHBOOK, supra note 2, instr. 7-8-1.

[lxxi] Diaz, 61 M.J. at 608.

[lxxii] *Id.* at 609 (citing United States v. Yarborough, 18 M.J. 452, 457 (C.M.A. 1984)).

[lxxiii] *Id.* This instruction was consistent with Instruction 7-8-3 of the BENCHBOOK.

[lxxiv] See MCM, supra note 41, MIL. R. EV*ID.* 404(a)(1).

[lxxv] *See id.* MIL. R. EV*ID.* 608(a).

[lxxvi] 61 M.J. 425 (2005).

[lxxvii] *Id.* at 427; see MCM, supra note 41, para. 37c(5); BENCHBOOK, supra note 2, instr. 3-37-2d.

[lxxviii] Brewer, 61 M.J. at 430. It appears that the military judge drew these instructions (with the exception of the last paragraph) directly from the MCM. MCM, supra note 41, para. 37c(5). The majority opinion states that these instructions were taken "almost verbatim" from the Benchbook. Although the above instruction also appears in the Benchbook (with the exception of the italicized language), as the dissent correctly notes, the instructions are nearly verbatim from the MCM.

[lxxix] Brewer, 61 M.J. at 432.

[lxxx] *Id.* at 431.

[lxxxi] *Id.*
[lxxxii] BENCHBOOK, supra note 2, instr. 3-37-2d.

[lxxxiii] 61 M.J. 30 (2005)

[lxxxiv] The case indicates that the defense did intend on calling one witness, but when the government objected to that witness' testimony, the defense decided not to call the witness and rested at the close of the government's case. *Id.* at 32.

[lxxxv] *Id.*

[lxxxvi] BENCHBOOK, supra note 2, instr. 7-12. The defense did not object to the propriety of the trial counsel's comments and the military judge did not further address them.

[lxxxvii] Carter, 61 M.J. at 33.

[lxxxviii] *Id.* (citing 2003 CCA LEXIS 257).

[lxxxix] *Id.* at 31.

[xc] *Id.* at 34.

[xci] "Trial counsel may not argue the prosecution's evidence is unrebutted if the only rebuttal could come from the accused." MCM, supra note 41, R.C.M. 919(b) Discussion.

[xcii] As the CAAF noted, "[o]nly [the accused] possessed information to contradict the Government's sole witness." Carter, 61 M.J. at 34.

[xciii] Failure to do so results in the appellate courts evaluating the issue under a plain error analysis – distinctly less favorable to the accused than had the issue been preserved by objection.

[xciv] Although the Benchbook does not have a single instruction addressing all these issues for use by the military judge in situations such as these, the Benchbook does address these issues thus: The accused has an absolute right to remain silent (BENCHBOOK, supra note 2, instr. 7-12); The accused is presumed not guilty until proven otherwise by the government (BENCHBOOK, supra note 2, sec. V, paras. 2-5 and 2-5-12); and The government carries the burden of proof and the burden never shifts to the defense (*Id.*). Although the members would have heard each of these instructions by the end of trial, the military judge could remind the members of these instructions should the situation dictate.

[xcv] The CAAF implies that had the military judge repeated his instruction to the members regarding the accused's right to remain silent after the trial counsel's closing argument, the result may have been different: "Although the military judge instructed the members that they were not to make adverse inferences from [the accused's] decision to remain silent, we agree with the majority opinion below that trial counsel's subsequent rebuttal [argument] vitiated any curative effect." Carter, 61 M.J. at 35.

[xcvi] 62 M.J. 175 (2005).

[xcvii] *Id.* at 178.

[xcviii] Appendix I to the Court's opinion contains the entire findings argument by the government.

[xcix] Fletcher, 62 M.J. at 185.

[c] *Id.*

[ci] See BENCHBOOK, supra note 2, sec. V, para. 2-5-9.

[cii] The CAAF specifically said the military judge "should have interrupted trial counsel before [s]he ran the full course of [her] impermissible argument. Corrective instructions at an early point might have dispelled the taint of the initial remarks." Fletcher, 62 M.J. at 185 (quoting United States v. Knickerbocker, 2 M.J. 128, 129 (C.M.A. 1977)).

[ciii] 61 M.J. 354 (2005).

[civ] BENCHBOOK, supra note 2, instr. 7-12.

[cv] The military judge did not make a record of specific concerns that caused him to give the instruction, other than a generalized concern that the members might hold the accused's failure to testify against him. Although the military judge told counsel that he would not give the instruction last, he d*id.* When that error was pointed out by the defense after instructions, the military judge admitted the error was his. However, he denied a request for mistrial.

[cvi] United States v. Forbes, 59 M.J. 934 (N-M. Ct. Crim. App. 2004).

[cvii] *Id.* at 939.

[cviii] Forbes, 61 M.J. at 358.

[cix] *Id.* at 359.

[cx] *Id.* at 355-56.

[cxi] *Id.* at 356.

[cxii] Rule 301(g) and the Drafter's Analysis for MRE 301(g), which makes it clear that the intent is to "leave[] that decision solely within the hands of the defense . . . in all but the most unusual circumstances." MCM, supra note 41, MIL. R. EV*ID.* 301(g).

[cxiii] *Id.*

[cxiv] Forbes, 61 M.J. at 357.

[cxv] *Id.* at 359.

[cxvi] *Id.* at 360.

[cxvii] The factors included should go beyond the potential—that arguably exists in every case—that the members might "hold it against the accused" if he did not testify. For example, if questions from the members repeatedly indicate a desire to hear from the accused or repeatedly question why the accused did not testify, such an instruction may be necessary, over defense objection, "in the interests of justice."

[cxviii] 60 M.J. 727 (Army Ct. Crim. App. 2004).

[cxix] *Id.* at 742.

[cxx] *Id.*

[cxxi] *Id.*

[cxxii] BENCHBOOK, supra note 2, instr. 7-12.

[cxxiii] The ACCA cited United States v. Mobley, 31 M.J. 273, 279 (C.M.A. 1990) ("It is black letter law that a trial counsel [or military judge] may not comment directly, indirectly, or by innuendo, on the fact that an accused did not testify in his defense."). Andreozzi, 60 M.J. at 742.

[cxxiv] 61 M.J. 482 (2005).

[cxxv] *Id.*

[cxxvi] 53 M.J. 800 (A.F. Ct. Crim. App. 2000).

[cxxvii] Barrier, 61 M.J. at 483. Although an instruction of similar import currently exists in the BENCHBOOK, supra note 2, sec. V, para. 2-5-23, the military judge's instruction here was much more detailed.

[cxxviii] *Id.* at 484 (citing United States v. Grill, 48 M.J. 131, 133 (1998)).

[cxxix] *Id.* at n.2.

[cxxx] *Id.*

[cxxxi] *Id.*

[cxxxii] *Id.* at 484.

[cxxxiii] *Id.* at 486.

[cxxxiv] United States v. Grill, 48 M.J. 131 (1998). Judge Crawford said she "mourn[s the Court's] . . . missed opportunity to clarify, modify, or overrule this Court's opinion in United States v. Grill. . . ." Barrier, 61 M.J. at 486. Many may agree. Citing United States v. Mamaluy, 10 C.M.R. 102 (C.M.A. 1959), the Barrier majority said "It has long been the rule of law that the sentences in other cases cannot be given to court-martial members for comparative purposes." Query: If that has always been the case, why was the military judge reversed in Grill?

[cxxxv] 62 M.J. 31 (2005).

[cxxxvi] *Id.* at 37.

[cxxxvii] *Id.* at 38.

[cxxxviii] *Id.* at 37.

[cxxxix] The CAAF eschewed the common term "impeachment of the verdict" in favor of the term relitigation of the findings. *Id.* at 37 n.2.

[cxl] 62 M.J. 150 (2005).

[cxli] *Id.* at 151.

[cxlii] *Id.*

[cxliii] *Id.*

[cxliv] *Id.* at 152 (citing United States v. Mamaluy, 10 C.M.R. 102 (C.M.A. 1959)).

[cxlv] One might think that such information would clearly be allowed under Grill – in fact, the CAAF reversed the military judge in Grill for failing to allow the accused to include arguably similar information in his unsworn statement: that "no charges have ever been brought against [a civilian co-accused], and may never be brought against him." United States v. Grill, 48 M.J. 131, 132 (1998). However, following its framework for analysis from Johnson, the CAAF in Sowell characterized the comment as appropriate rebuttal based on the facts of this case – not generally appropriate, as they did for the comment in Grill.

[cxlvi] "Ordinarily, such information might properly be viewed in context as impeaching the member's findings. As the Court of Criminal Appeals concluded, . . . Mamaluy remain[s] good law. However, we conclude under the limited circumstances of this case, that the Government's argument on findings opened the door to proper rebuttal. . . ." Sowell, 62 M.J. at 152.