CYBERSECURITY

- A MAJOR NATIONAL NEED

- A MAJOR OPPORTUNITY FOR UMD

- A SOURCE OF FUNDS

- A SOURCE OF FRIENDS/PARTNERS

- AN IMPORTANT RESEARCH AND EDUCATION FOCUS

Michael Wertheimer

Michael Wertheimer

Professor of the Practice
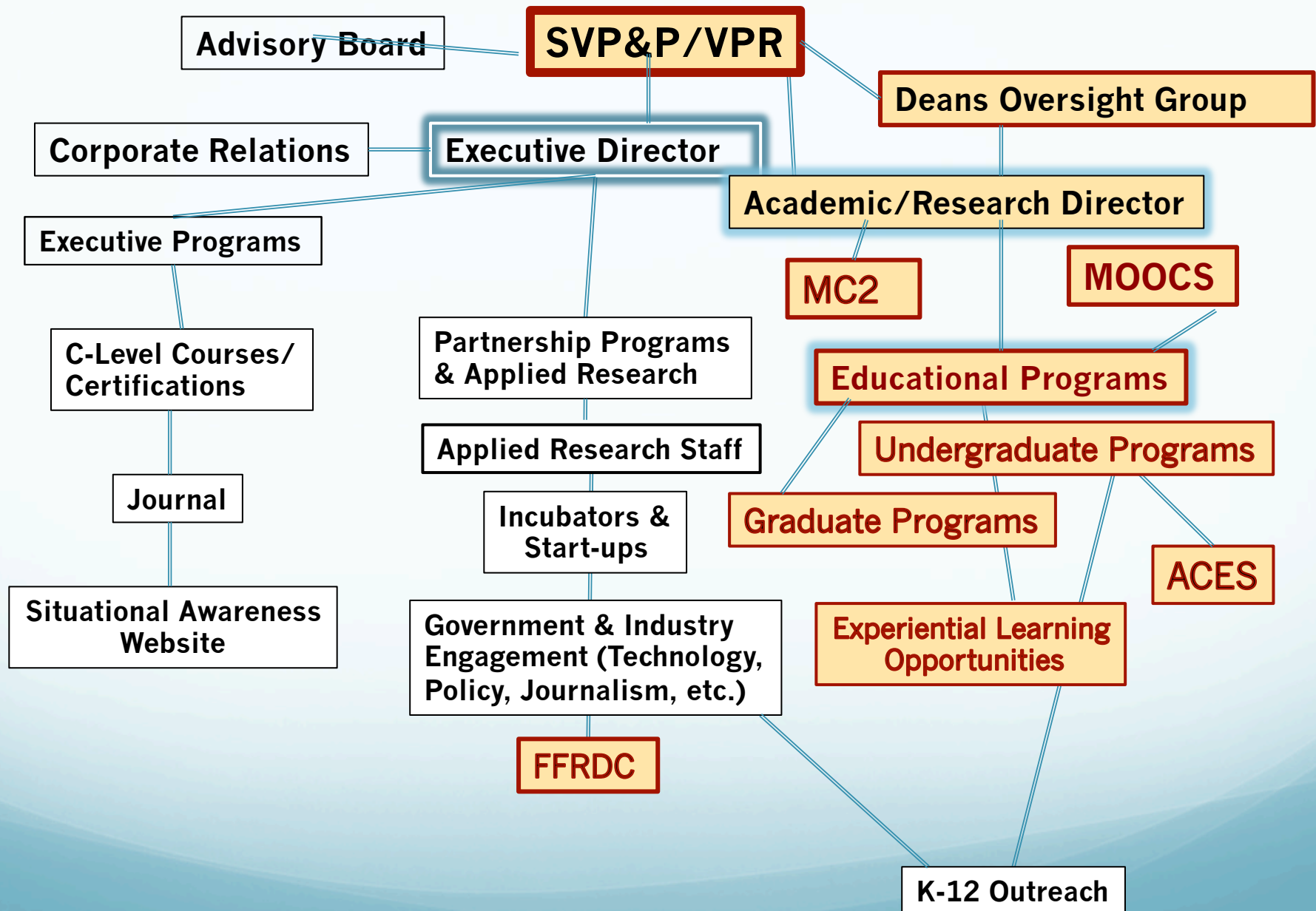
2202C Van Munching Hall

mwerthei@umd.edu

301-405-3988

Wertheimer joins UMD from the National Security Agency, where he served as director of research from 2010-2014. In 2009 he was selected as Technical Director for the Data Acquisition Office in the NSA's Signals Intelligence Directorate.
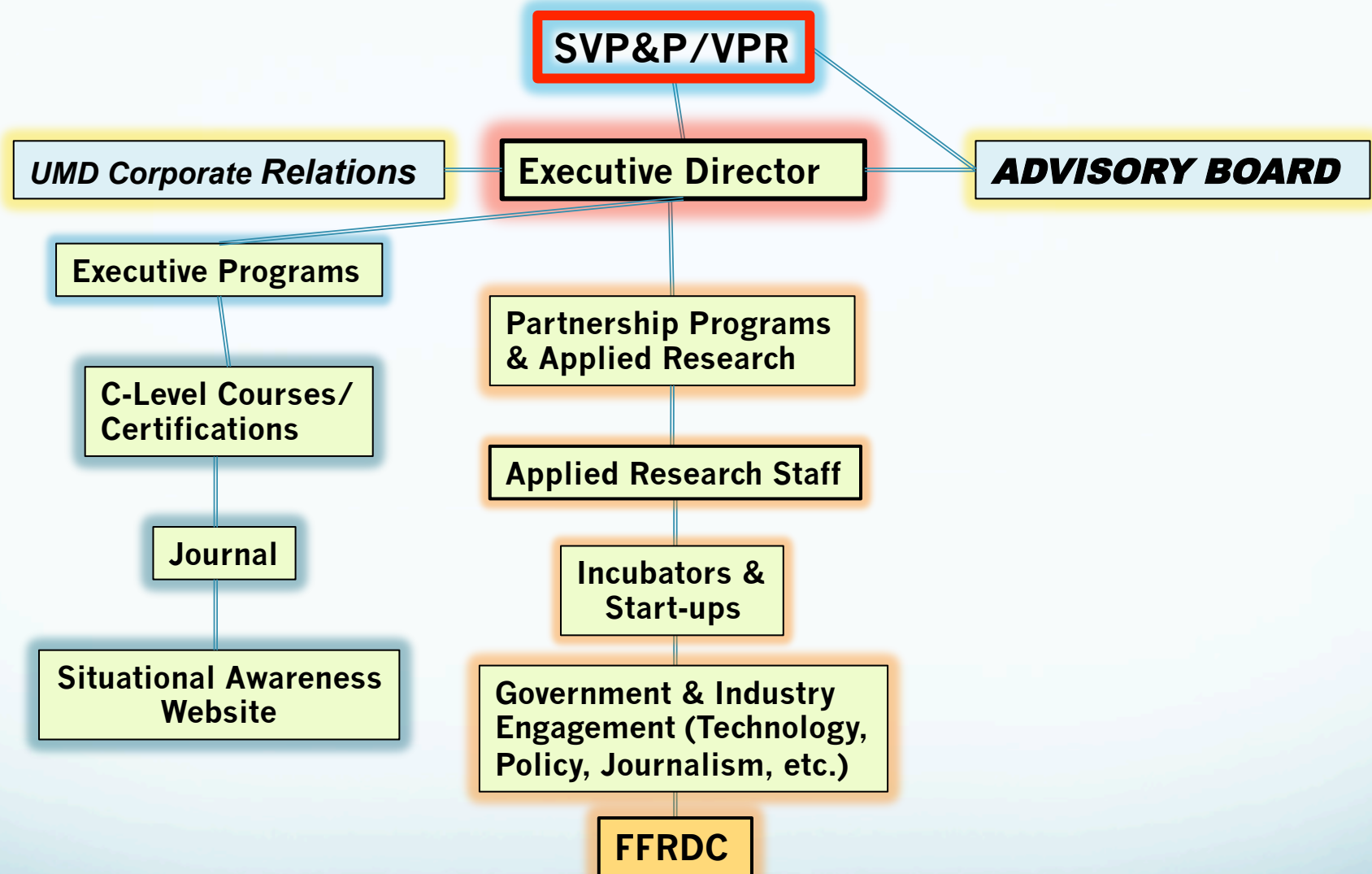
Prior to that, he was the assistant deputy director and chief technology officer of the Office of the Director of National Intelligence for Analysis. Wertheimer oversaw the coordination of intelligence community efforts to bring increased depth and accuracy to analysis through technology.

Wertheimer spent two years in industry building a research group focused on the intelligence community. From 1982 to 2003 he was a cryptologic mathematician at the National Security Agency where he trained in the design and analysis of cryptology with special emphasis on cryptanalysis digital signals processing, reverse engineering, software development, supercomputing and algorithm optimization.

Wertheimer received his PhD and MA in mathematics from the University of Pennsylvania. He received BA degrees in mathematics and philosophy from the University of Rochester.

Maryland Global Institute for Cybersecurity

Advisory Board

SVP&P/VPR

Deans Oversight Group

Corporate Relations

Executive Director

Academic/Research Director

Executive Programs

MC2

MOOCS

C-Level Courses/ Certifications

Partnership Programs & Applied Research

Educational Programs

Undergraduate Programs

Applied Research Staff

Journal

Graduate Programs

Incubators & Start-ups

ACES

Situational Awareness Website

Government & Industry Engagement (Technology, Policy, Journalism, etc.)

Experiential Learning Opportunities

FFRDC

K-12 Outreach

Executive Programs

From "internal escalation" to "patch implementation," cybersecurity is a field abounding in technical jargon. MGIC executive programs will help leaders and decision-makers "cut through the gibberish," offering superior CEO and C-suite education and certification.

- C-LEVEL COURSES AND PROGRAMS
  - Courses in cybersecurity as it relates to the boardroom, including applied practices and principles
  - Executive master's degree in cybersecurity
  - Access to national thought leadership in the field, including access to policy positions and participation in roundtables on topics affected by cybersecurity
  - Discussions with government and industry partners through forums and simulations focused on cybersecurity challenges in different industry verticals
- MARYLAND CYBER JOURNAL
  - A national "business review" for cyber, this online journal will feature plain language case studies and coverage of events and topics that industry and government leaders can apply on a daily basis.
- MARYLAND CYBER WATCH
  - This daily briefing will provide the latest in overnight cyber-threat updates, translated into actionable suggestions and presented in prose accessible and impactful to a CEO.
  - Industry-leading Web journals digested into a moderated "news clips" format
  - Macro-level cyber activity summarized on a daily, weekly and monthly basis, Established with an Information Sharing and Analysis Center (ISAC) model for the university and its partners

Partner Programs and Applied Research

The Maryland Global Institute for Cybersecurity (MGIC) will leverage the university's strengths in research and entrepreneurship to deliver timely, affordable and effective cybersecurity solutions for industry and government partners.

- **INNOVATION DISTRICT INITIATIVE**
  - **MGIC will make space available for partners to work side by side with University of Maryland students and faculty—even enabling companies to do R&D on campus with their own employees.**
- **RESEARCH**
  - **Dedicated institute research staff**
  - **Partner access to campus research facilities and talent**
  - **Corporate and government partnerships for applied cyber research opportunities with near-term commercial capabilities**
- **INNOVATION/COMMERCIALIZATION**
  - **Regular industry roundtables to focus on areas of innovation for university resources**
  - **A core set of grand challenges to be met through commercialization of R&D, such as developing the first securitizations of .umd.edu and .md.us**
  - **Opportunities for students and researchers to creatively problem-solve grand challenges as part of their curriculum**

Partner Programs and Applied Research

- **GOVERNMENT & INDUSTRY PARTNERSHIPS**
  - **Joint opportunities in exercises, simulations and R&D Positions on topics related to cybersecurity at the state and federal level**
  - **Newsletter focused on cyber-threat data and potential implications, with scholarly articles on position and response**
- **INCUBATORS/STARTUPS**
  - **Campus- and consortium-wide opportunities to help commercialize ideas, research and solutions that focus on cybersecurity solutions**
  - **An MGIC startup venture fund**
  - **A licensing waiver for institute start-ups to encourage students and faculty to create new companies with intellectual property developed on campus**

QUESTIONS to address:

- **Relationship of work for others and restricted research to traditional research and education programs on campus**
    - **Do we need to identify off-campus space for these activities?**
    - **What is the campus perspective on doing restricted research—i.e., research in which the results can not be published without permission (note this is not work that requires a security clearance)**

- **What are the opportunities to incorporate the executive education curriculum in offerings for our own students**

- **Organizational Structure and oversight—do we need an over-arching Institute to present a coherent face to our supporters and stakeholders?**

- **Costs and funding opportunities**

- **How to connect with the FFRDC and K-12 opportunities**

Questions, continued

- How will this initiative will be structured to be collaborative, and in particular how the various cybersecurity curricula and activities already in place will be integrated with this new initiative?

- How is this going to connect to the Honors program in cybersecurity?

- Who is going to implement all the extra activity, and in particular to design and teach all the new courses, and how is this to be paid for?

- To what extent will information developed by the new initiative would be classified or commercially privileged, and how that fits with the initiative being a core part of the university (or if it pushes it to being an affiliated but separate institute).

- Some concern about how these initiatives are aligned with our core mission of training undergraduate and graduate students.