

**NRL BAA Announcement  
# 55-09-06**



**Mathematical Foundations of High Assurance Computing**

The Formal Methods Section (Code 5543) of the Naval Research Laboratory's Center for High Assurance Computer Systems is seeking white papers for innovative research in the mathematics underlying security and high assurance computing. For white papers accepted and approved by Code 5543, submitters will be requested to submit formal BAA proposals to the Contracting Division at NRL.

Current and anticipated areas of research focus include:

1. Cryptographic Protocol Design and Analysis – We are interested in the analysis of security protocols for security and performance. Design of new protocols, together with their analysis, is also of interest. Analysis techniques may include formal methods, mathematical analysis, simulation, and experimental evaluation.
2. Information Hiding – We are interested in the mathematical, and in particular, information theoretic analysis of covert communication channels, steganography, watermarking, and related areas of information hiding and concealed knowledge. In addition, we are interested in the mathematics underlying pragmatic security solutions for possible collaborative research. Appropriate theoretical models from other areas, such as spike trains from the biosciences, are also of current research interest.
3. Anonymous Communication – We are interested in the design and analysis of traffic-security through anonymous and route-trusted communications. Emphasis will be placed on metrics and definitions for traffic security, cryptographic building blocks, network topology and structure, routing protocols, performance, usability, and secure distribution of network information. Techniques can be based on mathematical analysis, simulation and/or experimentation.
4. Informatic Phenomena – This area focuses on the mathematical structure of information, both qualitative and quantitative, and uses it to study various issues related to the secure transfer of information. New paradigms on information, such as quantum information, are of particular interest, including their reconciliation with relativistic notions. The primary mathematical techniques employed will be domain theory and other forms of topological algebra.

5. Mathematical and Logical Analysis of Distributed Systems – We are interested in mathematics and logics that are integrated with design methodologies for producing secure distributed systems. Emphasis will be placed on hardware-software codesign, distributed architectures, and programming methodologies. The formal apparatus will include non-standard logics (modal, substructural, etc.), category theory, domain theory, Shannon information theory, and structures that relate these elements in an elegant and coherent manner.

Address White Papers (WP) to Code 5543, or [email](#), telephone (202) 404-8888. Allow one month before requesting confirmation of receipt of WP, if confirmation is desired. Substantive contact should not take place prior to evaluation of a WP by NRL. If necessary, NRL will initiate substantive contact.