Approved for release by NSA on 12-01-2011, Transparency Case# 63852

UNCLASSIFIED

(U) Cryptologic Almanac 50th Anniversary Series

(U) Dr. Lowell K. Frazer

(U) Dr. Lowell K. ("Jim") Frazer was the founder of modern cryptographic evaluation. As a result of his efforts, all cryptography used for classified applications by the U.S. Department of Defense and intelligence community is now subject to a rigorous scientific evaluation. His contributions and influence had tremendous impact on the Agency's core discipline, cryptomathematics, and on the COMSEC/ INFOSEC/Information Assurance mission. He influenced the design of virtually every U.S. cryptographic system fielded before 1990 and was instrumental in maintaining a qualified preeminence for U.S. COMSEC. In addition to instituting this revolutionary change, Dr. Frazer was a prolific producer of technical papers.

(U) In 1939 Dr. Frazer graduated from high school at the age of 14 and started at Indiana University. He returned IU after World War II, finished his master's degree, and received his Ph.D. in 1951. Immediately after, Dr. Frazer went to work for what is now NSA.

(U) During his early years at the Agency, he was selected as the first COMSEC mathematician assigned as an integrated member in H Group at GCHQ from 1954 to 1956. During this two-year tour, he performed assessments on seven U.S. and U.K. cryptographic systems, designed two U.K. speech cryptosystems, and discovered an analytic technique that would be used to attack a wide range of cipher machines over the next three decades. Also, he authored a primer for use in training new COMSEC cryptomathematicians. On the SIGINT side, he was responsible for the analysis and initial break of several diverse systems.

(U) Perhaps his most important single contribution to cryptology was his ingenuity in framing the standards for judging the robustness of INFOSEC products. Dr. Frazer was the principal formulator of the standards the U.S. and the U.K. use to judge the strength of cryptographic systems, and he continued to lead the adaptation and extension of those standards as the role of cryptography grew from COMSEC to the more diverse INFOSEC mission. Almost fifty years later, the standards rationale and motivation and the "costing" methodology remain valid.

(U) Under his leadership, the Industrial TEMPEST Program, a novel approach to government-industry interaction matured. The program was created to allow industry to develop TEMPEST-suppressed information processors for government agencies. More importantly, he integrated TEMPEST concerns into the overall security evaluation process

for U.S. cryptographic equipment. This integration has allowed significantly expanded analytic resources to be shared by TEMPEST and general signal analytic concerns. He led the development of one of the Agency's finest signal analytic facilities where none existed previously.

(U) Dr. Frazer played a major role in the development of the mathematics, cryptanalysis, and INFOSEC communities in NSA. He served on an advisory group which reviewed the mathematics courses offered by the National Cryptologic School and was associated with the CryptoMath Institute (CMI) from its inception and served as its president. In fact, Dr. Frazer was elected as a Distinguished Member of the CMI and the Kryptos Society. He was a member of the Mathematics, Cryptanalysis, and COMSEC Career Panels and was an advisor to the NSA Technical Journal for approximately twenty years. Dr. Frazer was a continual conduit of ideas and cooperation with the SIGINT community and came to be known as "Mr. COMSEC Math."

(U) Dr. Frazer received numerous awards throughout his career, including the Agency's Meritorious Civilian Service Award in 1969 and the Exceptional Civilian Service Award in 1981. In addition, he was awarded the DCI's National Intelligence Distinguished Service Medal in 1985.