(AIG Letterhead)

May 21, 2012

VIA EDGAR CORRESPONDENCE

Mr. Jeffrey P. Riedler
Assistant Director
Securities and Exchange Commission
Division of Corporation Finance
100 F Street, NE
Mail Stop 4720
Washington, D.C. 20549

Re: American International Group, Inc.
Form 10-K for the Fiscal Year Ended December 31, 2011
Filed on February 23, 2012
File No. 001-08787

Dear Mr. Riedler:

We are in receipt of your letter dated May 9, 2012 with respect to American International Group, Inc.'s ("AIG") Annual Report on Form 10-K for the fiscal year ended December 31, 2011 ("Form 10-K"). This letter sets forth AIG's response to the Staff's comment contained in your letter.

AIG acknowledges that the adequacy and accuracy of the disclosure in the Form 10-K is the responsibility of AIG, that Staff comments or changes to disclosure in response to Staff comments do not foreclose the Securities and Exchange Commission (the "Commission") from taking any action with respect to the Form 10-K and that Staff comments may not be asserted by AIG as a defense in any proceeding initiated by the Commission or any person under the Federal securities laws of the United States.

We have repeated your comment below to facilitate your review.

* * * * *

Risk Factors

If we are unable to maintain the availability of our electronic data systems and safeguard the security of our data…, page 41

1. **In response to our prior comment 2, you state that you have experienced threats to your data and systems, including malware and computer virus attacks, unauthorized access, systems failures and disruptions. In order to place the risks described in this risk factor in an appropriate context, please expand your risk factor to state that you have experienced threats to your data and systems, including malware and computer virus attacks, unauthorized access, systems failures and disruptions.**

AIG Response

Pursuant to the Staff's comment, AIG will expand its risk factor on electronic data systems and the handling of confidential information in its Quarterly Report on Form 10-Q for the quarterly period ended June 30, 2012 to read in its entirety as follows (expanded disclosure is underlined):

> *If we are unable to maintain the availability of our electronic data systems and safeguard the security of our data, our ability to conduct business may be compromised, which could adversely affect our consolidated financial condition or results of operations.* We use computer systems to store, retrieve, evaluate and utilize customer, employee, and company data and information. Some of these systems in turn, rely upon third-party systems. Our business is highly dependent on our ability to access these systems to perform necessary business functions, including providing insurance quotes, processing premium payments, making changes to existing policies, filing and paying claims, administering variable annuity products and mutual funds, providing customer support and managing our investment portfolios. Systems failures or outages could compromise our ability to perform these functions in a timely manner, which could harm our ability to conduct business and hurt our relationships with our business partners and customers. In the event of a natural disaster, a computer virus, a terrorist attack or other disruption inside or outside the U.S., our systems may be inaccessible to our employees, customers or business partners for an extended period of time, and our employees may be unable to perform their duties for an extended period of time if our data or systems are disabled or destroyed. Our systems could also be subject to unauthorized access, such as physical or electronic break-ins or unauthorized tampering. Like other global companies, we have, from time to time, experienced threats to our data and systems, including malware and computer virus attacks, unauthorized access, systems failures and disruptions. AIG maintains cyber risk insurance, but this insurance may not cover all costs associated with the consequences of personal, confidential or proprietary information being compromised. In some cases, such unauthorized access may not be immediately detected. This may impede or interrupt our business operations and could adversely affect our consolidated financial condition or results of operations.
>
> In addition, we routinely transmit, receive and store personal, confidential and proprietary information by email and other electronic means. Although we attempt to keep such information confidential, we may be unable to do so in all events, especially with clients, vendors, service providers, counterparties and other third parties who may not have or use appropriate controls to protect confidential information. Furthermore, certain of our businesses are subject to compliance with laws and regulations enacted by U.S. federal and state governments, the European Union or other jurisdictions or enacted by various regulatory organizations or exchanges relating to the privacy and security of the information of clients, employees or others. The compromise of personal, confidential or proprietary information could result in remediation costs, legal liability, regulatory action and reputational harm.

* * * * *

If you have any questions or require any additional information, please do not hesitate to contact me at (212) 770-5123.

Very truly yours,

/s/ Kathleen E. Shannon
Kathleen E. Shannon
Senior Vice President
and Deputy General Counsel